NUMERICAL SEMIGROUPS
&
KUNZ POLYTOPES

OSAKA UNIVERSITY
AUGUST 2018

Introduction

Introduction

Question:

In how many ways can we remove g positive integers from $\mathbb{N}_0$ so that the remaining set is additively closed?

Introduction

Question:

In how many ways can we remove g positive integers from $\mathbb{N}_0$ so that the remaining set is additively closed?

Answer:

I don't know!

Introduction

- A numerical semigroup is an additive sub-monoid of $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ whose complement is finite.

Introduction

- A numerical semigroup is an additive sub-monoid of $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ whose complement is finite.
- The genus of S is the number of gaps, i.e. the cardinality of its complement.

Introduction

- A numerical semigroup is an additive sub-monoid of $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ whose complement is finite.
- The genus of S is the number of gaps, i.e. the cardinality of its complement.
- The multiplicity of S is the smallest nonzero element in S.

Introduction

- A numerical semigroup is an additive sub-monoid of $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ whose complement is finite.
- The genus of S is the number of gaps, i.e. the cardinality of its complement.
- The multiplicity of S is the smallest nonzero element in S.
- The embedding dimension of S is the size of its minimal generating set.

Introduction

- A numerical semigroup is an additive sub-monoid of $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ whose complement is finite.
- The genus of S is the number of gaps, i.e. the cardinality of its complement.
- The multiplicity of S is the smallest nonzero element in S.
- The embedding dimension of S is the size of its minimal generating set.
- The Frobenius number of S is the largest number NOT in S.

Example

Example

$S = \{0,3,6,8,9,11,12,14,15,16,\ldots\}$

$= \mathbb{N}_0 \setminus \{1,2,4,5,7,10,13\}$

$= \langle 3,8 \rangle$

Example

$S = \{0,3,6,8,9,11,12,14,15,16,\ldots\}$

$= \mathbb{N}_0 \setminus \{1,2,4,5,7,10,13\}$

$= < 3,8 >$

$g(S) = 7$

Example

$S = \{0,3,6,8,9,11,12,14,15,16,\ldots\}$

$= \mathbb{N}_0 \setminus \{1,2,4,5,7,10,13\}$

$= < 3,8 >$

$g(S) = 7$

$m(S) = 3$

Example

$S = \{0,3,6,8,9,11,12,14,15,16,\ldots\}$

$= \mathbb{N}_0 \setminus \{1,2,4,5,7,10,13\}$

$= < 3,8 >$

$g(S) = 7$

$m(S) = 3$

$F(S) = 13$

Example

$S = \{0,3,6,8,9,11,12,14,15,16,\ldots\}$

$= \mathbb{N}_0 \setminus \{1,2,4,5,7,10,13\}$

$= \langle 3,8 \rangle$

$g(S) = 7$

$m(S) = 3$

$F(S) = 13$

$e(S) = 2$

Applications

Applications

- **Diophantine Equations:**
  Nonnegative integer solutions to equations of the form $a_1x_1 + \ldots + a_nx_n = b$, where $a_1,\ldots,a_n$ and b are natural numbers with gcd $(a_1,\ldots,a_n) = 1$

Applications

- **Diophantine Equations:**
  Nonnegative integer solutions to equations of the form $a_1x_1 + \ldots + a_nx_n = b$, where $a_1,\ldots,a_n$ and b are natural numbers with gcd $(a_1,\ldots,a_n) = 1$

- **Commutative Algebra:**
  Families of numerical semigroups yielding complete intersection and thus Gorenstein semigroup rings of the form $K[t^a : a \text{ in } S]$

Applications

- **<u>Diophantine Equations:</u>**
  Nonnegative integer solutions to equations of the form $a_1x_1 + \ldots + a_nx_n = b$, where $a_1,\ldots,a_n$ and b are natural numbers with gcd $(a_1,\ldots,a_n) = 1$

- **<u>Commutative Algebra:</u>**
  Families of numerical semigroups yielding complete intersection and thus Gorenstein semigroup rings of the form $K[t^a : a \text{ in } S]$

- **<u>Algebraic Geometry:</u>**
  The local intersection multiplicities of formal power series form a numerical semigroup under some conditions

Applications

- **Algebraic Codes:**
  Classification of Weierstrass numerical semigroups in coding theory and cryptography

Applications

- **Algebraic Codes:**
  Classification of Weierstrass numerical semigroups in coding theory and cryptography

- **Moreover:**
  Factorization of monoids
  Singularities of plane algebraic curves
  One-dimensional analytically irreducible local domains
  etc…

The Problem

The Problem

Combinatorial Question:

In how many ways can we remove g positive integers from $\mathbb{N}_0$ so that the remaining set is additively closed?

The Problem

Combinatorial Question:

In how many ways can we remove g positive integers from $\mathbb{N}_0$ so that the remaining set is additively closed?

Equivalently:

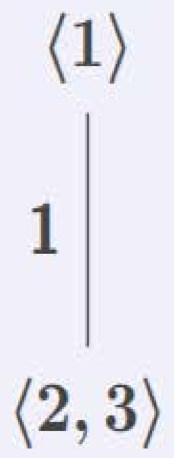
What is the number N(g) of numerical semigroups with genus g?

Tree Structure

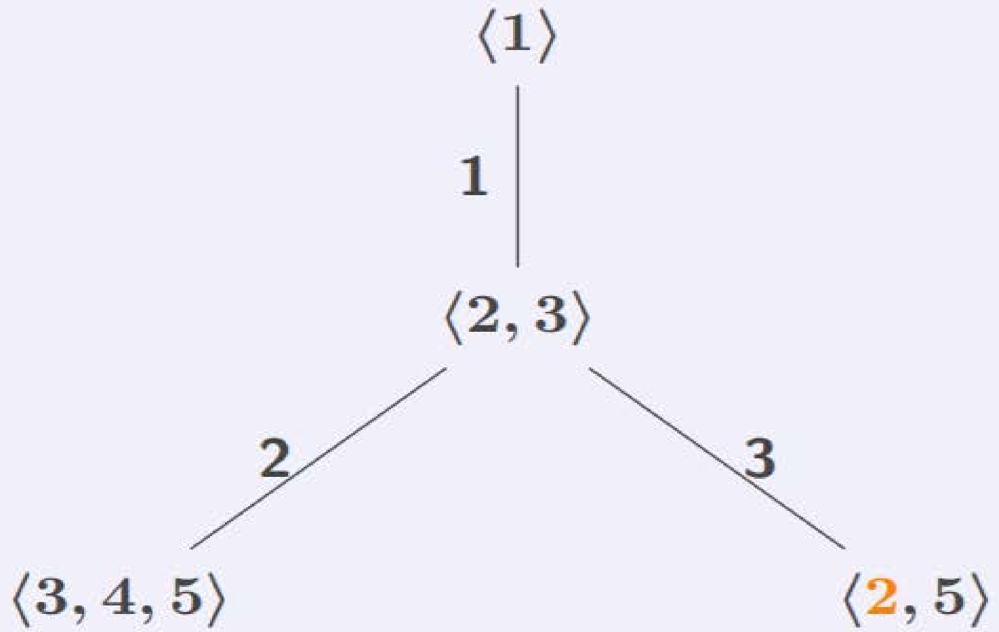
Tree Structure

$$\langle 1 \rangle$$

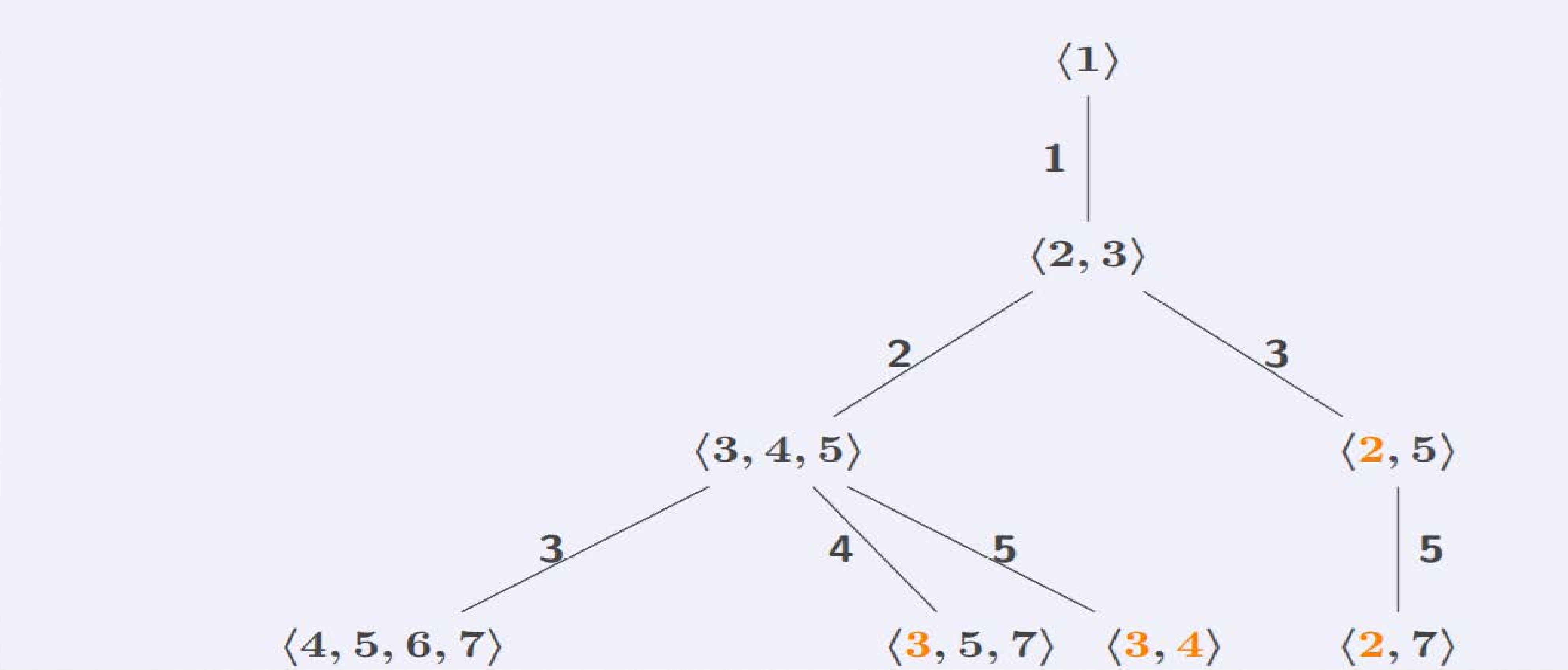
Tree Structure



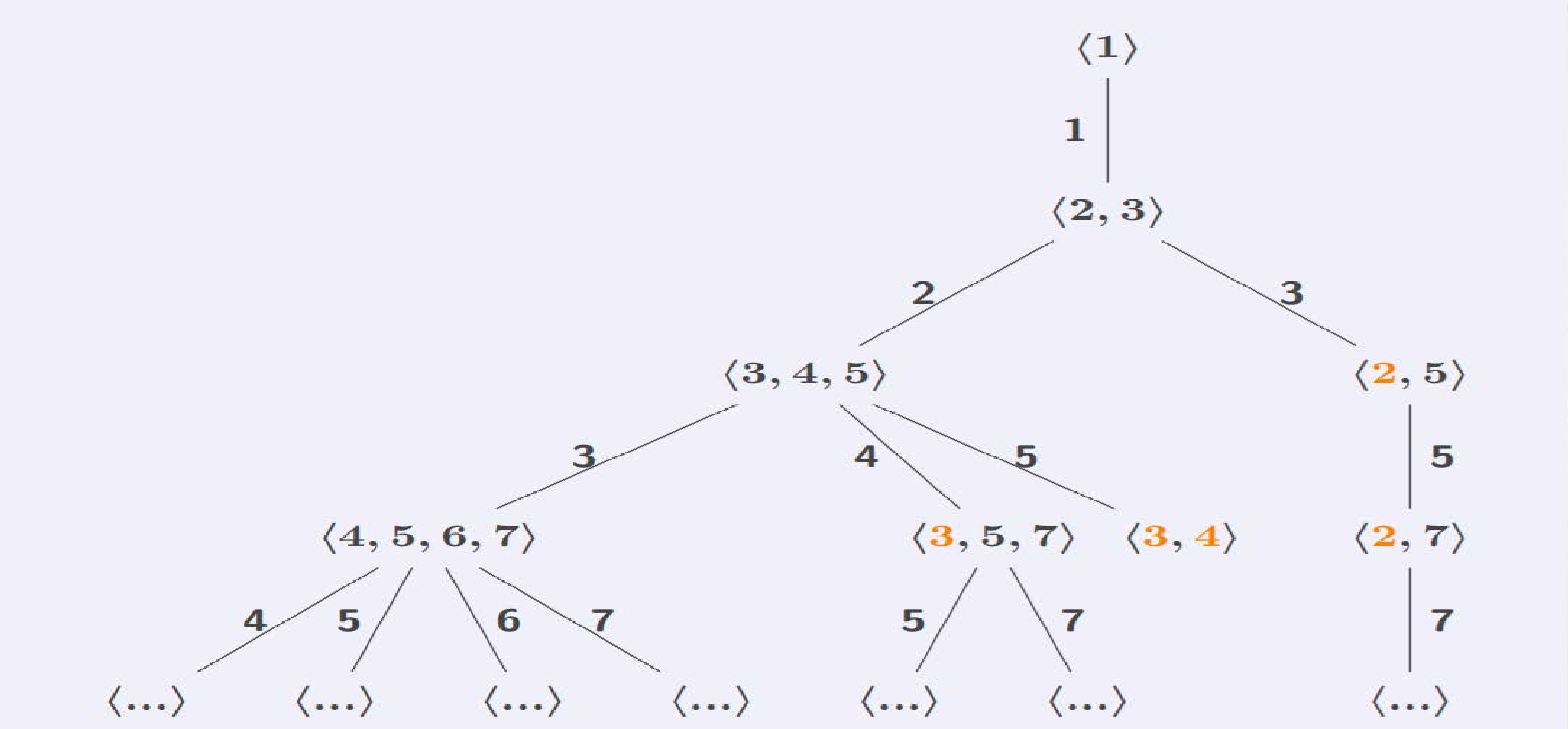
Tree Structure



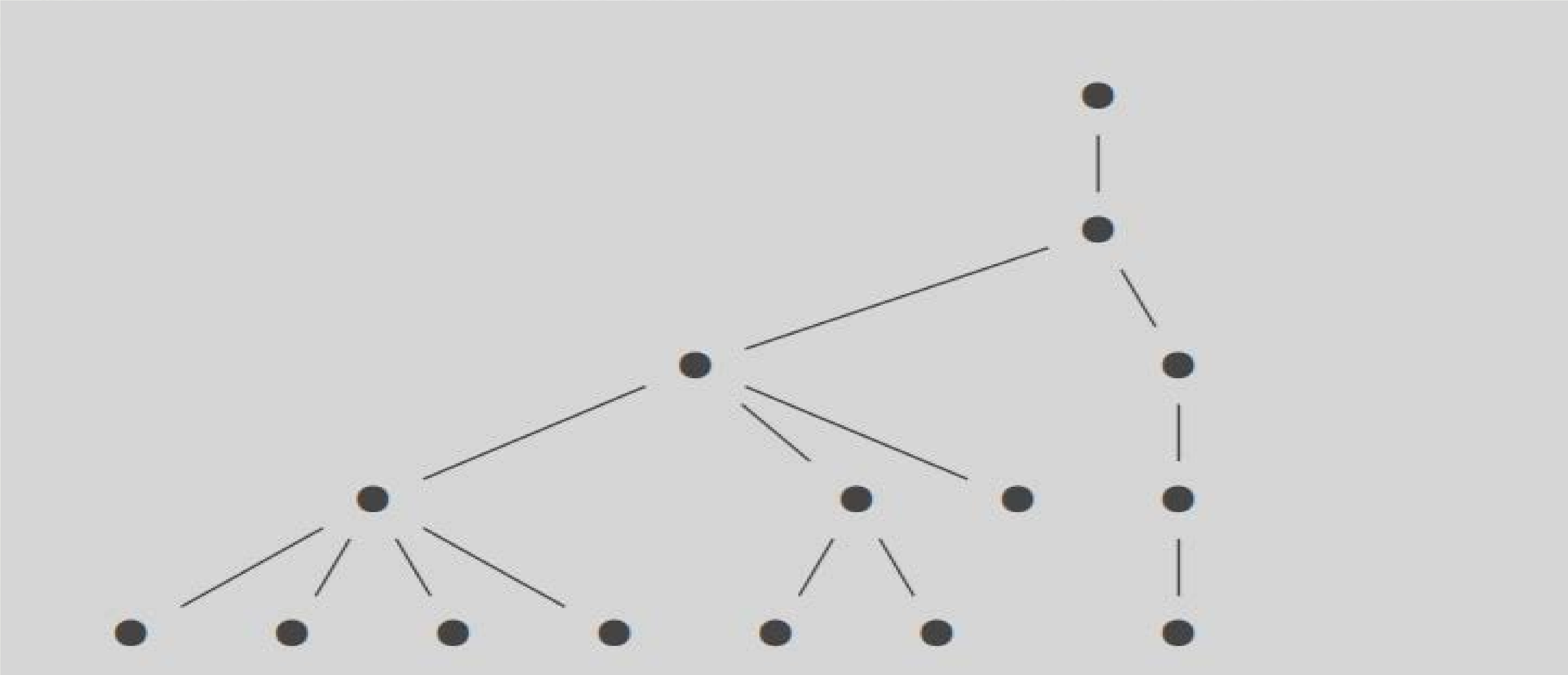
Tree Structure



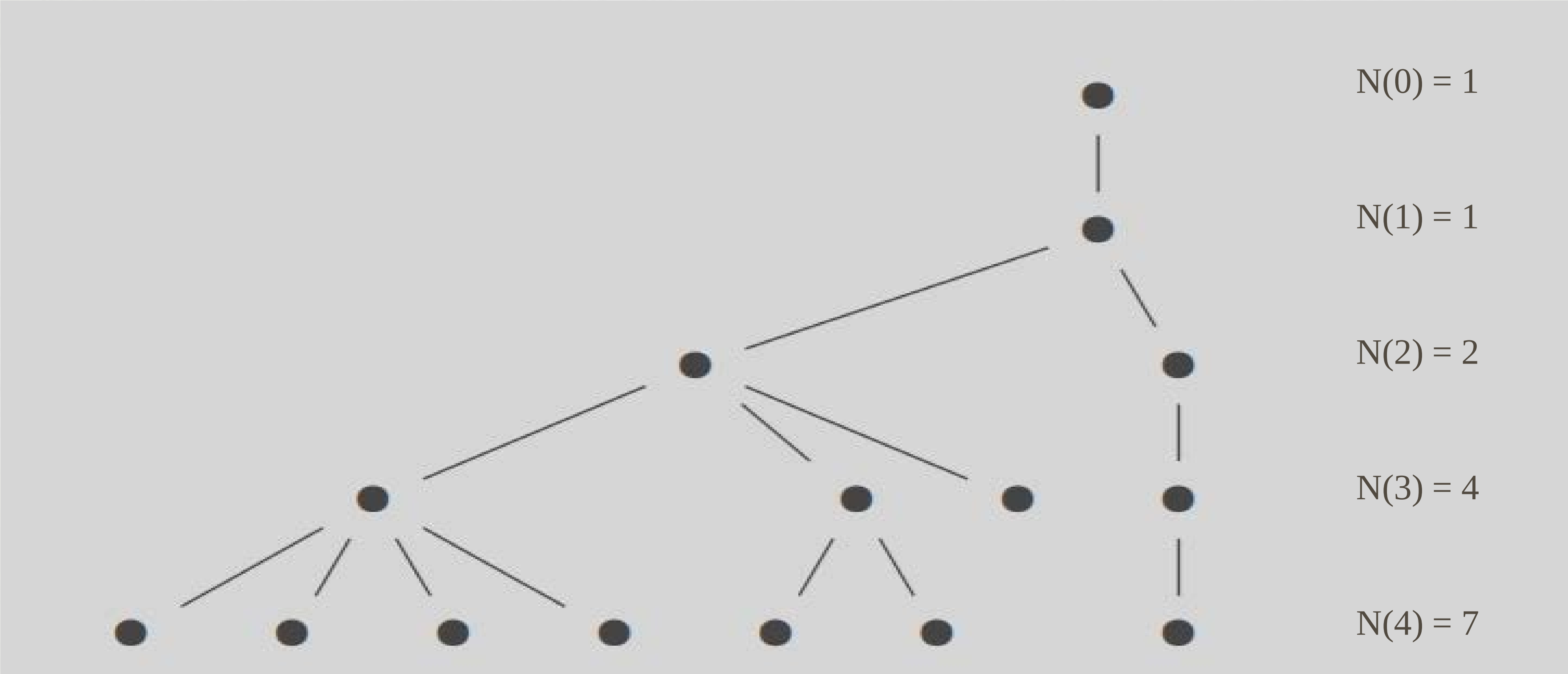
Tree Structure



Tree Structure



Tree Structure



Numerical Computation

Numerical Computation

- N(10) = 204
- N(20) = 37,396
- N(30) = 5,646,773
- N(40) = 774,614,284
- N(50) = 101,090,300,128
- N(67) = 377,866,907,506,273

Bounds

Bounds

- **Bras Amoros `08:**

$$N(g) \leq \frac{1}{g+1}\binom{2g}{g}$$

Bounds

- **Bras Amoros `08:**

$$N(g) \leq \frac{1}{g+1}\binom{2g}{g}$$

- **Bras Amoros `08, Elizalde `10:**

$$F_{g+2} - 1 \leq N(g) \leq 1 + 3.2^{g-3}$$

Asymptotical Behavior

Asymptotical Behavior

- **Conjecture (Bras-Amoros `08):**

1) $\lim_{g\to\infty} \frac{N(g-1)+N(g-2)}{N(g)} = 1$

2) $\lim_{g\to\infty} \frac{N(g)}{N(g-1)} = \varphi$, the golden ratio.

Asymptotical Behavior

- **Conjecture (Bras-Amoros `08):**

1) $\lim_{g\to\infty} \frac{N(g-1)+N(g-2)}{N(g)} = 1$

2) $\lim_{g\to\infty} \frac{N(g)}{N(g-1)} = \varphi$, the golden ratio.

- **Theorem (Zhai `13):**

$\lim_{g\to\infty} \frac{N(g)}{\varphi^g} = K$ for some constant K,

Asymptotical Behavior

- **Conjecture (Bras-Amoros `08):**

1) $\lim_{g\to\infty} \frac{N(g-1)+N(g-2)}{N(g)} = 1$

2) $\lim_{g\to\infty} \frac{N(g)}{N(g-1)} = \varphi$, the golden ratio.

- **Theorem (Zhai `13):**

$\lim_{g\to\infty} \frac{N(g)}{\varphi^g} = K$ for some constant K, hence 1) and 2) hold.

Nonetheless…

Nonetheless…

- **<u>Strong Genus Conjecture:</u>**

  $N(g) \geq N(g-1) + N(g-2)$ for all $g \geq 2$

Nonetheless…

- **Strong Genus Conjecture:**

  $N(g) \geq N(g-1) + N(g-2)$ for all $g \geq 2$

- **Weak Genus Conjecture:**

  $N(g) \geq N(g-1)$ for all $g \geq 1$

Apéry Sets

Apéry Sets

- Let S be a numerical semigroup with multiplicity m. The Apéry set of S with respect to m is defined as

  Ap(S,m) = {0, w(1), w(2),…, w(m-1)},

  where $w(i) = k_i\, m + i$ is the smallest element in S that is congruent to i mod m.

Apéry Sets

- Let S be a numerical semigroup with multiplicity m. The Apéry set of S with respect to m is defined as

  Ap(S,m) = {0, w(1), w(2),…, w(m-1)},

  where $w(i) = k_i m + i$ is the smallest element in S that is congruent to i mod m.

- <u>**Theorem (Selmer `77):**</u>

  1) $g(S) = k_1 + k_2 + \ldots + k_{m-1}$

Apéry Sets

- Let S be a numerical semigroup with multiplicity m. The Apéry set of S with respect to m is defined as

  Ap(S,m) = {0, w(1), w(2),…, w(m-1)},

  where $w(i) = k_i\, m + i$ is the smallest element in S that is congruent to i mod m.

- **Theorem (Selmer `77):**

  1) $g(S) = k_1 + k_2 + \ldots + k_{m-1}$

  2) F(S) = max [Ap(S,m)] – m

From N(g) to N(m,g)

From N(g) to N(m,g)

- Let N(m,g) be the number of numerical semigroups with genus g and multiplicity m.

From N(g) to N(m,g)

- Let N(m,g) be the number of numerical semigroups with genus g and multiplicity m. Clearly, N(g) = N(1,g) + N(2,g) + … + N(g,g) + N(g+1,g).

From N(g) to N(m,g)

- Let N(m,g) be the number of numerical semigroups with genus g and multiplicity m. Clearly, N(g) = N(1,g) + N(2,g) + … + N(g,g) + N(g+1,g).

- **Theorem (Kunz `87, Rosales et al. `02):**

  There is a one-to-one correspondence between the set of numerical semigroups of genus g and multiplicity m and the integer points satisfying the following conditions:

$$x_i \geq 1, \quad \text{for all } i = 1,2,\ldots,m-1$$
$$x_i + x_j - x_{i+j} \geq 0 \quad \text{for all } 1 \leq i \leq j \leq m-1 \ \&\ i+j \leq m-1$$
$$x_i + x_j - x_{i+j-m} \geq -1 \quad \text{for all } 1 \leq i \leq j \leq m-1 \ \&\ i+j \geq m+1$$

From N(g) to N(m,g)

- Let N(m,g) be the number of numerical semigroups with genus g and multiplicity m. Clearly, N(g) = N(1,g) + N(2,g) + … + N(g,g) + N(g+1,g).

- **<u>Theorem (Kunz `87, Rosales et al. `02):</u>**

  There is a one-to-one correspondence between the set of numerical semigroups of genus g and multiplicity m and the integer points satisfying the following conditions:

$$x_i \geq 1, \qquad \text{for all } i = 1,2,\ldots,m-1$$
$$x_i + x_j - x_{i+j} \geq 0 \qquad \text{for all } 1 \leq i \leq j \leq m-1 \;\&\; i+j \leq m-1$$
$$x_i + x_j - x_{i+j-m} \geq -1 \qquad \text{for all } 1 \leq i \leq j \leq m-1 \;\&\; i+j \geq m+1$$
$$x_1 + \ldots + x_{m-1} = g$$

From N(g) to N(m,g) to MED(m,g)

From N(g) to N(m,g) to MED(m,g)

- Let MED(m,g) be the number of maximal embedding dimension numerical semigroups with genus g and multiplicity m, i.e. e(S) = m(S).

From N(g) to N(m,g) to MED(m,g)

- Let MED(m,g) be the number of maximal embedding dimension numerical semigroups with genus g and multiplicity m, i.e. e(S) = m(S).
  Clearly, MED(g) = MED(1,g) + MED(2,g) + … + MED(g,g) + MED(g+1,g).

From N(g) to N(m,g) to MED(m,g)

- Let MED(m,g) be the number of maximal embedding dimension numerical semigroups with genus g and multiplicity m, i.e. e(S) = m(S).
  Clearly, MED(g) = MED(1,g) + MED(2,g) + … + MED(g,g) + MED(g+1,g).

- **Theorem (Kunz `87, Rosales et al. `02):**

  There is a one-to-one correspondence between the set of maximal embedding dimension numerical semigroups of genus g and multiplicity m and the integer points satisfying the following conditions:

$$x_i \geq 1, \qquad \text{for all } i = 1,2,\ldots,m-1$$
$$x_i + x_j - x_{i+j} \geq 1 \qquad \text{for all } 1 \leq i \leq j \leq m-1 \text{ \& } i+j \leq m-1$$
$$x_i + x_j - x_{i+j-m} \geq 0 \qquad \text{for all } 1 \leq i \leq j \leq m-1 \text{ \& } i+j \geq m+1$$
$$x_1 + \ldots + x_{m-1} = g$$

Polyhedral Structure

Polyhedral Structure

- Let P_N be the polytope corresponding to N(m,g) and P_{MED} the polytope corresponding to MED(m,g). Define P to be the polytope satisfying the same inequalities with 0 on the right hand side.

Polyhedral Structure

- Let P_N be the polytope corresponding to N(m,g) and P_{MED} the polytope corresponding to MED(m,g). Define P to be the polytope satisfying the same inequalities with 0 on the right hand side.
- Clearly, $P_{MED} \subseteq P \subseteq P_N$ and they all are (m – 2)-dimensional.

Polyhedral Structure

- Let P_N be the polytope corresponding to N(m,g) and P_{MED} the polytope corresponding to MED(m,g). Define P to be the polytope satisfying the same inequalities with 0 on the right hand side.
- Clearly, $P_{MED} \subseteq P \subseteq P_N$ and they all are (m – 2)-dimensional.
- Embedding the last equation into the previous inequalities, we can write these polytopes in the form $A.x \geq b(g)$ where A is a matrix with integer entries and b is a vector whose coordinates are linear functions in terms of g. We mention some of the properties of P_N:

Polyhedral Structure

1) The matrix A has $\left\lfloor \frac{m^2-1}{2} \right\rfloor$ rows.

Polyhedral Structure

1) The matrix A has $\left\lfloor \frac{m^2-1}{2} \right\rfloor$ rows.

2) The coordinates of b(g) belong to the set {0,1,-1,g,-g+1,-g-1,-2g-1}.

Polyhedral Structure

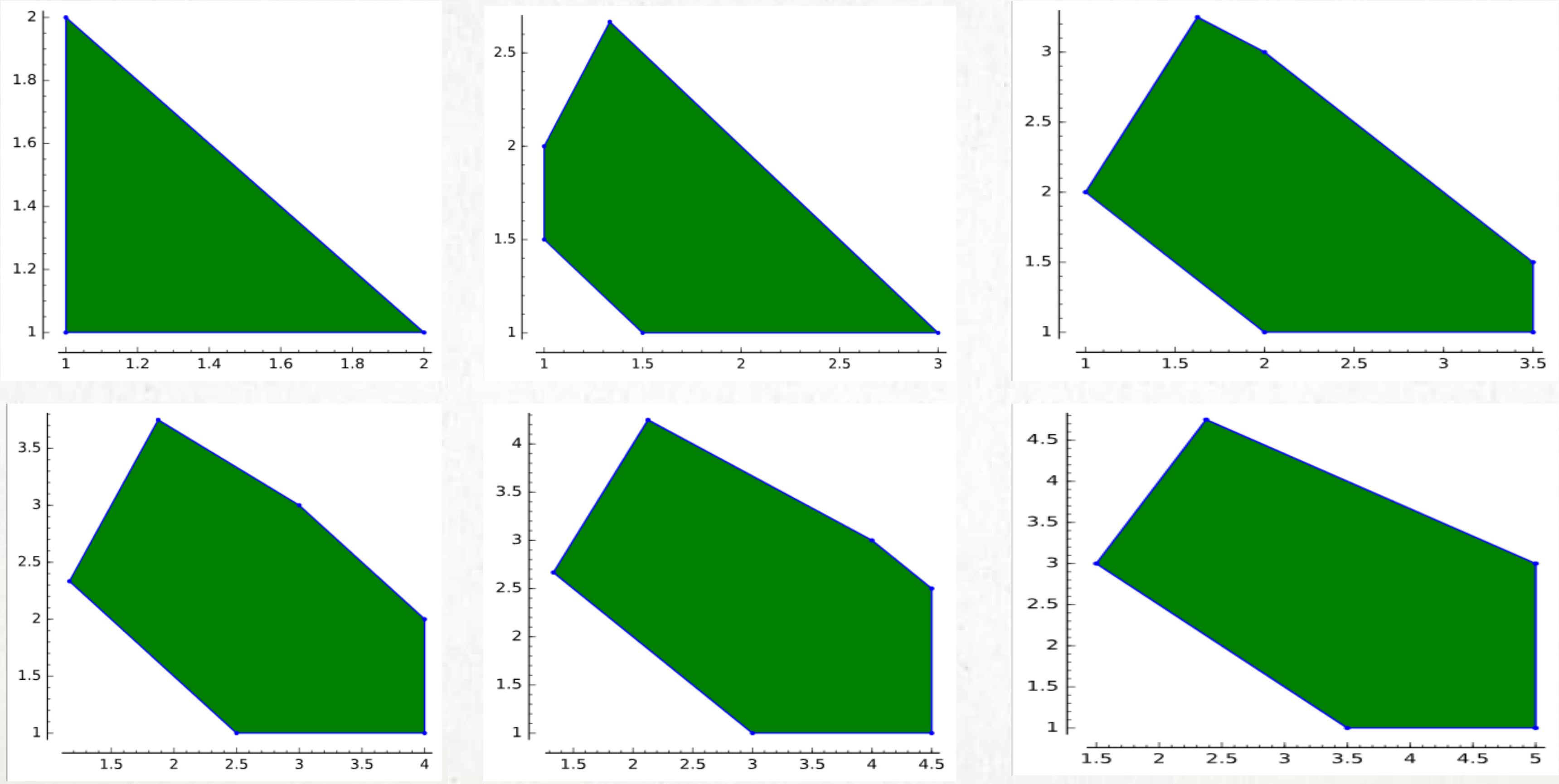
1) The matrix A has $\left\lfloor \frac{m^2-1}{2} \right\rfloor$ rows.

2) The coordinates of b(g) belong to the set {0,1,-1,g,-g+1,-g-1,-2g-1}.

3) For $g \geq (m-1)^2$, the polytope P "stabilizes", i.e. φ(m) inequalities become redundant.

The Case m = 4

The Case m = 4



1 1.2 1.4 1.6 1.8 2
1 1.5 2 2.5
1 1.5 2 2.5 3
1 1.5 2 2.5 3 3.5
1.5 2 2.5 3 3.5 4
1 1.5 2 2.5 3 3.5
1.5 2 2.5 3 3.5 4 4.5
1 1.5 2 2.5 3 3.5 4
1.5 2 2.5 3 3.5 4 4.5 5
1 1.5 2 2.5 3 3.5 4 4.5

Combinatorial Structure

Combinatorial Structure

- Let p(g) be the number of integer points in P.
  Since $P_{MED} \subseteq P \subseteq P_N$, it follows that $MED(m,g) \leq p(g) \leq N(m,g)$

Combinatorial Structure

- Let p(g) be the number of integer points in P.
  Since $P_{MED} \subseteq P \subseteq P_N$, it follows that $MED(m,g) \leq p(g) \leq N(m,g)$

- **Theorem (Kaplan `12):**
  For fixed m, N(m,g) agrees eventually with a quasipolynomial in g of degree m – 2, with period depending on m. The same holds for MED(m,g).

Combinatorial Structure

- Let p(g) be the number of integer points in P.
  Since $P_{MED} \subseteq P \subseteq P_N$, it follows that MED(m,g) $\leq$ p(g) $\leq$ N(m,g)

- **Theorem (Kaplan `12):**
  For fixed m, N(m,g) agrees eventually with a quasipolynomial in g of degree m – 2, with period depending on m. The same holds for MED(m,g).

- **Theorem (Blanco et al. `11):**
  For fixed m, N(m,g) and MED(m,g) can be computed in polynomial time.
  Consequently, the same holds for N(g) and MED(g).

Combinatorial Structure

- **Theorem:**

$$\lim_{g\to\infty} \frac{N(m,g)}{g^{m-2}} = \lim_{g\to\infty} \frac{MED(m,g)}{g^{m-2}} = Vol(P).$$

Combinatorial Structure

- **Theorem:**

$$\lim_{g\to\infty}\frac{N(m,g)}{g^{m-2}}=\lim_{g\to\infty}\frac{MED(m,g)}{g^{m-2}}=Vol(P).$$

- For small values of m, the volume of P is computed:

$$\frac{1}{3},\frac{1}{12},\frac{1}{135},\frac{71}{81{,}648},\frac{1{,}633}{36{,}288{,}000},\frac{12{,}256{,}093}{3{,}923{,}023{,}104{,}000},\ldots$$

Combinatorial Structure

- <u>**Theorem:**</u>

$$N(m,g) \leq MED(m, g + m - 1) \text{ for all } g \geq 0 \text{ and } m \geq 2.$$

Combinatorial Structure

- **Theorem:**

$N(m,g) \leq MED(m, g + m - 1)$ for all $g \geq 0$ and $m \geq 2$.

Equality holds when m is prime and $g > \frac{(m-1)(m-2)}{2}$.

The Case m = 4 (continued)

The Case m = 4 (continued)

$$N(4,g) = \begin{cases} \frac{g^2}{12} + \frac{g}{2} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{7}{12} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{1}{3} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{1}{4} \end{cases}$$

The Case m = 4 (continued)

$$N(4,g) = \begin{cases} \frac{g^2}{12} + \frac{g}{2} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{7}{12} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{1}{3} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{1}{4} \end{cases} \qquad MED(4,g) = \begin{cases} \frac{g^2}{12} \\ \frac{g^2}{12} - \frac{1}{12} \\ \frac{g^2}{12} - \frac{1}{3} \\ \frac{g^2}{12} + \frac{1}{4} \end{cases}$$

The Case m = 4 (continued)

$$N(4,g) = \begin{cases} \frac{g^2}{12} + \frac{g}{2} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{7}{12} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{1}{3} \\ \frac{g^2}{12} + \frac{g}{2} - \frac{1}{4} \end{cases} \quad MED(4,g) = \begin{cases} \frac{g^2}{12} \\ \frac{g^2}{12} - \frac{1}{12} \\ \frac{g^2}{12} - \frac{1}{3} \\ \frac{g^2}{12} + \frac{1}{4} \end{cases} \quad p(g) = \begin{cases} \frac{g^2}{12} + \frac{5g}{12} + 1 \\ \frac{g^2}{12} + \frac{g}{12} - \frac{1}{6} \\ \frac{g^2}{12} + \frac{5g}{12} - \frac{1}{6} \\ \frac{g^2}{12} + \frac{g}{12} \\ \frac{g^2}{12} + \frac{g}{12} + \frac{1}{2} \\ \frac{g^2}{12} + \frac{5g}{12} + \frac{1}{2} \\ \frac{g^2}{12} + \frac{g}{12} - \frac{2}{3} \\ \frac{g^2}{12} + \frac{5g}{12} + \frac{1}{3} \end{cases}$$

Special Results

Special Results

- $N(4,g)$ = number of partitions of $g + 6$ into 3 parts such that the i^{th} part is greater than i

Special Results

- N(4,g) = number of partitions of g + 6 into 3 parts such that the i^{th} part is greater than i

- MED(4,g) = number of partitions of g + 3 into 3 distinct parts.

Future Directions

Future Directions

- **<u>Strong & Weak Genus Conjectures:</u>**

  $N(g) \geq N(g-1) + N(g-2)$ for all $g \geq 2$ & $N(g) \geq N(g-1)$ for all $g \geq 1$

Future Directions

- **Strong & Weak Genus Conjectures:**

  $N(g) \geq N(g-1) + N(g-2)$ for all $g \geq 2$ & $N(g) \geq N(g-1)$ for all $g \geq 1$

- **Nondecreasing Sequences:**

  $N(m,g) \geq N(m,g-1)$ & $MED(m,g) \geq MED(m,g-1)$ for all $m \geq 2$

Future Directions

- **Strong & Weak Genus Conjectures:**

  $N(g) \geq N(g-1) + N(g-2)$ for all $g \geq 2$ & $N(g) \geq N(g-1)$ for all $g \geq 1$

- **Nondecreasing Sequences:**

  $N(m,g) \geq N(m,g-1)$ & $MED(m,g) \geq MED(m,g-1)$ for all $m \geq 2$

- **Other types of numerical semigroups:**

  One can define symmetric, pseudo-symmetric, Arf, irreducible, saturated, etc… numerical semigroups and ask the same questions!!
  What properties does a 'generic' numerical semigroup have, for large g???

Future Directions

g\m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	N(g)
0	1																										1
1		1																									1
2		1	1																								2
3		1	2	1																							4
4		1	2	3	1																						7
5		1	2	4	4	1																					12
6		1	3	6	7	5	1																				23
7		1	3	7	10	11	6	1																			39
8		1	3	9	13	17	16	7	1																		67
9		1	4	11	16	27	28	22	8	1																	118
10		1	4	13	22	37	44	44	29	9	1																204
11		1	4	15	24	49	64	72	66	37	10	1															343
12		1	5	18	32	66	85	116	116	95	46	11	1														592
13		1	5	20	35	85	112	172	188	182	132	56	12	1													1001
14		1	5	23	43	106	148	239	288	304	277	178	67	13	1												1693
15		1	6	26	51	133	191	325	409	492	486	409	234	79	14	1											2857
16		1	6	29	61	163	237	441	559	754	796	763	587	301	92	15	1										4806
17		1	6	32	68	196	301	573	750	1094	1246	1282	1172	821	380	106	16	1									8045
18		1	7	36	80	236	369	737	1015	1534	1841	2074	2045	1759	1122	472	121	17	1								13467
19		1	7	39	89	282	444	945	1334	2106	2601	3227	3356	3217	2580	1502	578	137	18	1							22464
20		1	7	43	104	330	541	1193	1737	2840	3561	4812	5301	5401	4976	3702	1974	699	154	19	1						37396