Apéry sets and Hilbert Series for Almost Arithmetic Semigroups

J.L. Ramírez Alfonsín

I3M,
Université Montpellier 2

1 Introduction

2 Hilbert series and Apéry set

3 Symmetry

4 Further work

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

We denote by $\langle a_1, \ldots, a_n \rangle$ the numerical semigroup generated by $a_1, \ldots, a_n$.

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

We denote by $\langle a_1, \ldots, a_n \rangle$ the numerical semigroup generated by $a_1, \ldots, a_n$.

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

We denote by $\langle a_1, \ldots, a_n \rangle$ the numerical semigroup generated by $a_1, \ldots, a_n$.

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

We denote by $\langle a_1, \ldots, a_n \rangle$ the numerical semigroup generated by $a_1, \ldots, a_n$.

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

We denote by $\langle a_1, \ldots, a_n \rangle$ the numerical semigroup generated by $a_1, \ldots, a_n$.

Diophantine Frobenius Problem

Let $a_1, \ldots, a_n$ be positive integers with $\gcd(a_1, \ldots, a_n) = 1$, find the largest integer (called the Frobenius number and denoted by $g(a_1, \ldots, a_n)$) that is not representable as a nonnegative integer combination of $a_1, \ldots, a_n$.

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $g(3, 8) = 13$.

We denote by $\langle a_1, \ldots, a_n \rangle$ the numerical semigroup generated by $a_1, \ldots, a_n$.

Ideas

- Graph theory
- Discrete Optimisation problems (Knapsack problem)
- Additive number theory
- Index of primitivity of matrix
- Geometry of numbers (covering radius)
- Quantifier elimination
- Ehrhar polynomial
- Hilbert series
- Möbius function

Theorem (Sylvester, 1882) $g(a,b) = ab - a - b$.

Theorem (R.A., 1996) Computing $g(a_1, \ldots, a_n)$ is $\mathcal{NP}$-hard.

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Sylvester, 1882) $g(a, b) = ab - a - b$.

Theorem (R.A., 1996) Computing $g(a_1, \ldots, a_n)$ is $\mathcal{NP}$-hard.

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Theorem (Sylvester, 1882) $g(a, b) = ab - a - b$.

Theorem (R.A., 1996) Computing $g(a_1, \ldots, a_n)$ is $\mathcal{NP}$-hard.

Theorem (Kannan, 1992) There is a polynomial time algorithm to compute $g(a_1, \ldots, a_n)$ when $n \geq 2$ is fixed.

Methods

For $n = 3$

- Selmer and Bayer, 1978
- Rødseth, 1978
- Davison, 1994
- Scarf and Shallcross, 1993

For $n \geq 4$

- Heap and Lynn, 1964
- Wilf, 1978
- Nijenhuis, 1979
- Greenberg, 1980
- Killingbergtø, 2000
- Einstein, Lichtblau, Strzebonski and Wagon, 2007
- Roune, 2008

Methods

For $n = 3$

- Selmer and Bayer, 1978
- Rødseth, 1978
- Davison, 1994
- Scarf and Shallcross, 1993

For $n \geq 4$

- Heap and Lynn, 1964
- Wilf, 1978
- Nijenhuis, 1979
- Greenberg, 1980
- Killingbergtø, 2000
- Einstein, Lichtblau, Strzebonski and Wagon, 2007
- Roune, 2008

Methods

For $n = 3$

- Selmer and Bayer, 1978
- Rødseth, 1978
- Davison, 1994
- Scarf and Shallcross, 1993

For $n \geq 4$

- Heap and Lynn, 1964
- Wilf, 1978
- Nijenhuis, 1979
- Greenberg, 1980
- Killingbergtø, 2000
- Einstein, Lichtblau, Strzebonski and Wagon, 2007
- Roune, 2008

Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon, 2007

Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second

Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Roune, 2008

Find $g(a_1, \ldots, a_4)$ involving $10,000$-digit numbers in few seconds

Find $g(a_1, \ldots, a_{13})$ involving 10-digit numbers in few days

Package

http ://www.broune.com/frobby/

http ://www.math.ruu.nl/people/beukers/frobenius/

http ://cmup.fc.up.pt/cmup/mdelgado/numericalsgps/

http ://reference.wolfram.com/mathematica/ref/FrobeniusNumber.html

Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon, 2007
Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second
Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Roune, 2008
Find $g(a_1, \ldots, a_4)$ involving 10, 000-digit numbers in few seconds
Find $g(a_1, \ldots, a_{13})$ involving 10-digit numbers in few days
Package
http ://www.broune.com/frobby/
http ://www.math.ruu.nl/people/beukers/frobenius/
http ://cmup.fc.up.pt/cmup/mdelgado/numericalsgps/
http ://reference.wolfram.com/mathematica/ref/FrobeniusNumber.html

Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon, 2007

Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second

Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Roune, 2008

Find $g(a_1, \ldots, a_4)$ involving 10, 000-digit numbers in few seconds

Find $g(a_1, \ldots, a_{13})$ involving 10-digit numbers in few days

Package

http ://www.broune.com/frobby/

http ://www.math.ruu.nl/people/beukers/frobenius/

http ://cmup.fc.up.pt/cmup/mdelgado/numericalsgps/

http ://reference.wolfram.com/mathematica/ref/FrobeniusNumber.html

Fast Algorithms (computational algebraic methods)

Einstein, Lichtblau, Strzebonski and Wagon, 2007

Find $g(a_1, \ldots, a_4)$ involving 100-digit numbers in about one second

Find $g(a_1, \ldots, a_{10})$ involving 10-digit numbers in two days

Roune, 2008

Find $g(a_1, \ldots, a_4)$ involving 10, 000-digit numbers in few seconds

Find $g(a_1, \ldots, a_{13})$ involving 10-digit numbers in few days

Package

http ://www.broune.com/frobby/

http ://www.math.ruu.nl/people/beukers/frobenius/

http ://cmup.fc.up.pt/cmup/mdelgado/numericalsgps/

http ://reference.wolfram.com/mathematica/ref/FrobeniusNumber.html

Hilbert series and Apéry set

Let $A[S] = K[z^{a_1}, \ldots, z^{a_n}]$ be the semigroup ring over K (of characteristic 0) associated to the semigroup $S = \langle a_1, \ldots, a_n \rangle$. Then, the Hilbert series of $A[S]$ is

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}$$

$$g(a_1, \ldots, a_n) = \text{degree of } H(A[S], z)$$

Theorem (Herzog 1970, Morales 1987) Formula for $H(A[S], z)$ when $S = \langle a, b, c \rangle$

Hilbert series and Apéry set

Let $A[S] = K[z^{a_1}, \ldots, z^{a_n}]$ be the semigroup ring over K (of characteristic 0) associated to the semigroup $S = \langle a_1, \ldots, a_n \rangle$. Then, the Hilbert series of $A[S]$ is

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}$$

$$g(a_1, \ldots, a_n) = \text{degree of } H(A[S], z)$$

Theorem (Herzog 1970, Morales 1987) Formula for $H(A[S], z)$ when $S = \langle a, b, c \rangle$

Hilbert series and Apéry set

Let $A[S] = K[z^{a_1}, \dots, z^{a_n}]$ be the semigroup ring over K (of characteristic 0) associated to the semigroup $S = \langle a_1, \dots, a_n \rangle$. Then, the Hilbert series of $A[S]$ is

$$H(A[S], z) = \sum_{i \in S} z^s = \frac{Q(z)}{(1 - z^{a_1}) \cdots (1 - z^{a_n})}$$

$$g(a_1, \dots, a_n) = \text{degree of } H(A[S], z)$$

Theorem (Herzog 1970, Morales 1987) Formula for $H(A[S], z)$

when $S = \langle a, b, c \rangle$

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S; m) = \{s \in S \mid s - m \notin S\}$$

$$S = Ap(S; m) + m\mathbb{Z}_{\geq 0}, \quad H(S; z) = \frac{1}{1 - z^m} \sum_{w \in Ap(S;m)} z^w$$

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $Ap(\langle 3, 8 \rangle; 3) = \{0, 8, 16\}$.

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S; m) = \{s \in S \mid s - m \notin S\}$$

$$S = Ap(S; m) + m\mathbb{Z}_{\geq 0}, \quad H(S; z) = \frac{1}{1 - z^m} \sum_{w \in Ap(S;m)} z^w$$

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 · · · · · ·

So, $Ap(\langle 3, 8 \rangle; 3) = \{0, 8, 16\}$.

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S;m) = \{s \in S \mid s - m \notin S\}$$

$$S = Ap(S;m) + m\mathbb{Z}_{\geq 0}, \quad H(S;z) = \frac{1}{1 - z^m} \sum_{w \in Ap(S;m)} z^w$$

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ······

So, $Ap(\langle 3, 8 \rangle; 3) = \{0, 8, 16\}$.

The *Apéry* set of $S = \langle a_1, \ldots, a_n \rangle$ for $m \in S$ is

$$Ap(S; m) = \{s \in S \mid s - m \notin S\}$$

$$S = Ap(S; m) + m\mathbb{Z}_{\geq 0}, \quad H(S; z) = \frac{1}{1 - z^m} \sum_{w \in Ap(S;m)} z^w$$

Example : If $a_1 = 3$ and $a_2 = 8$ then

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 $\cdots\cdots$

So, $Ap(\langle 3, 8\rangle; 3) = \{0, 8, 16\}$.

An almost arithmetic semigroup is generated by an almost arithmetic progression, $S = \langle a, a+d, a+2d, \ldots, a+kd, c\rangle$.

Let $s_{-1} = a$ and determine s_0 by

$$ds_0 \equiv c \pmod{s_{-1}}, \quad 0 \leq s_0 < s_{-1}.$$

If $s_0 \neq 0$, we use the Euclidean algorithm with negative division remainders,

$$\begin{aligned}
s_{-1} &= q_1 s_0 - s_1, & 0 \leq s_1 < s_0;\\
s_0 &= q_2 s_1 - s_2, & 0 \leq s_2 < s_1;\\
s_1 &= q_3 s_2 - s_3, & 0 \leq s_3 < s_2;\\
&\ldots & \\
s_{m-2} &= q_m s_{m-1} - s_m, & 0 \leq s_m < s_{m-1};\\
s_{m-1} &= q_{m+1} s_m, & 0 = s_{m+1} < s_m.
\end{aligned}$$

An almost arithmetic semigroup is generated by an almost arithmetic progression, $S = \langle a, a+d, a+2d, \ldots, a+kd, c\rangle$.

Let $s_{-1} = a$ and determine s_0 by

$$ds_0 \equiv c \pmod{s_{-1}}, \quad 0 \le s_0 < s_{-1}.$$

If $s_0 \neq 0$, we use the Euclidean algorithm with negative division remainders,

$$\begin{aligned}
s_{-1} &= q_1 s_0 - s_1, & 0 \le s_1 < s_0;\\
s_0 &= q_2 s_1 - s_2, & 0 \le s_2 < s_1;\\
s_1 &= q_3 s_2 - s_3, & 0 \le s_3 < s_2;\\
&\ldots\\
s_{m-2} &= q_m s_{m-1} - s_m, & 0 \le s_m < s_{m-1};\\
s_{m-1} &= q_{m+1} s_m, & 0 = s_{m+1} < s_m.
\end{aligned}$$

If $s_0 = 0$, we put $m = -1$. If $m \geq 0$, we have

$$\frac{s_{-1}}{s_0} = q_1 - \cfrac{1}{q_2 - \cfrac{1}{q_3 - \cfrac{1}{\ddots \; q_m - \cfrac{1}{q_{m+1}}}}}$$

which is known as the *Jung-Hirzebruch continued fraction* of s_{-1}/s_0.

We have $s_m = \gcd(a, c)$. We define integers P_i by $P_{-1} = 0$, $P_0 = 1$, and (if $m \geq 0$),

$$P_{i+1} = q_{i+1} P_i - P_{i-1}, \quad i = 0, \ldots, m.$$

Then, by induction on i,

$$s_i P_{i+1} - s_{i+1} P_i = a, \qquad i = -1, 0 \ldots, m,$$

and

$$-1 = P_{-1} < 0 = P_0 < \cdots < P_{m+1} = \frac{a}{s_m}.$$

In addition we have,

$$ds_i \equiv cP_i \pmod{a}, \quad i = -1, \ldots, m+1.$$

Putting

$$R_i = \frac{1}{a}\left((a+kd)s_i - kcP_i\right),$$

we then see that all the R_i are integers. Moreover, we have $R_{-1} = a + kd$, $R_0 = \frac{1}{a}((a+kd)s_0 - kc)$, and

$$R_{i+1} = q_{i+1}R_i - R_{i-1}, \quad i = 0, \ldots, m,$$

and again we see that all the R_i are integers. Furthermore,

$$-\frac{c}{s_m} = R_{m+1} < R_m < \cdots < R_0 < R_{-1} = a + kd,$$

so there is a unique integer v such that

$$R_{v+1} \leq 0 < R_v.$$

Theorem (Rødseth 1979) If $S = \langle a, a+d, a+2d, \ldots, a+kd, c\rangle$ then

$$Ap(S;a) = \left\{ a\left\lceil \frac{y}{k} \right\rceil + dy + cz \mid (y,z) \in A \cup B \right\}$$

where

$$A = \{(y,z) \in \mathbb{Z}^2 \mid 0 \le y < s_v - s_{v+1}, 0 \le z < P_{v+1}\},$$

$$B = \{(y,z) \in \mathbb{Z}^2 \mid 0 \le y < s_v, 0 \le z < P_{v+1} - P_v\}.$$

Theorem (R.A. and Rødseth, 2009) $S = \langle a, a+d, \ldots, a+kd, c\rangle$

$$H(S;x) = \frac{F_{s_v}(a;x)(1-x^{c(P_{v+1}-P_v)})+F_{s_v-s_{v+1}}(a;x)(x^{c(P_{v+1}-P_v)}-x^{cP_{v+1}})}{(1-x^a)(1-x^d)(1-x^{a+kd})(1-x^c)}$$

where

$$F_s(a;x) = (1-x^{a+kd})(1-x^{aq+ds}) - x^d(1-x^a)(1-x^{(a+kd)q})$$

with s a non-negative integer and $q = \lceil (s-1)/k \rceil$.

Corollary When $k = 1$ and $b = a + d$ we have that $S = \langle a, b, c \rangle$

$$H(S;x) = \frac{1 - x^{bs_v} - x^{cP_{v+1}} - x^{aR_v - R_{v+1}} + x^{aR_v + cP_{v+1}} + x^{bs_v - aR_{v+1}}}{(1-x^a)(1-x^b)(1-x^c)}$$

$$g(a,b,c) = \max\{aR_v + cP_{v+1}, bs_v - aR_{v+1}\} - a - b - c.$$

Corollary When $k = 1$ and $b = a + d$ we have that $S = \langle a, b, c\rangle$

$$H(S;x) = \frac{1 - x^{bs_v} - x^{cP_{v+1}} - x^{aR_v - R_{v+1}} + x^{aR_v + cP_{v+1}} + x^{bs_v - aR_{v+1}}}{(1 - x^a)(1 - x^b)(1 - x^c)}$$

$$g(a, b, c) = \max\{aR_v + cP_{v+1}, bs_v - aR_{v+1}\} - a - b - c.$$

Algorithm Apéry

Input : a, d, c, k, s_0 Output : $s_v, s_{v+1}, P_v, P_{v+1}$

$r_{-1} = a, r_0 = s_0$

$r_{i-1} = \kappa_{i+1} r_i + r_{i+1}, \kappa_{i+1} = \lfloor r_{i-1}/r_i \rfloor, 0 = r_{\mu+1} < r_\mu < \cdots < r_{-1}$

$p_{i+1} = \kappa_{i+1} p_i + p_{i-1}, \quad p_{-1} = 0, \quad p_0 = 1$

$T_{i+1} = -\kappa_{i+1} T_i + T_{i-1}, \quad T_{-1} = a + kd, T_0 = \frac{1}{a}((a+kd)r_0 - kc)$

IF there is a minimal u such that $T_{2u+2} \leq 0$, THEN

$$\begin{pmatrix} s_v & P_v \\ s_{v+1} & P_{v+1} \end{pmatrix} = \begin{pmatrix} \gamma & 1 \\ \gamma - 1 & 1 \end{pmatrix} \begin{pmatrix} r_{2u+1} & -p_{2u+1} \\ r_{2u+2} & p_{2u+2} \end{pmatrix}, \gamma = \left\lfloor \frac{-T_{2u+2}}{T_{2u+1}} \right\rfloor + 1$$

ELSE $s_v = r_\mu, s_{v+1} = 0, P_v = p_\mu, P_{v+1} = p_{\mu+1}$.

Algorithm Apéry

Input : a, d, c, k, s_0 Output : $s_v, s_{v+1}, P_v, P_{v+1}$

$r_{-1} = a, r_0 = s_0$

$r_{i-1} = \kappa_{i+1} r_i + r_{i+1}, \kappa_{i+1} = \lfloor r_{i-1}/r_i \rfloor, 0 = r_{\mu+1} < r_\mu < \cdots < r_{-1}$

$p_{i+1} = \kappa_{i+1} p_i + p_{i-1}, \quad p_{-1} = 0, \quad p_0 = 1$

$T_{i+1} = -\kappa_{i+1} T_i + T_{i-1}, \quad T_{-1} = a + kd, T_0 = \frac{1}{a}((a+kd)r_0 - kc)$

If there is a minimal u such that $T_{2u+2} \leq 0$, Then

$$\begin{pmatrix} s_v & P_v \\ s_{v+1} & P_{v+1} \end{pmatrix} = \begin{pmatrix} \gamma & 1 \\ \gamma - 1 & 1 \end{pmatrix} \begin{pmatrix} r_{2u+1} & -p_{2u+1} \\ r_{2u+2} & p_{2u+2} \end{pmatrix}, \gamma = \left\lfloor \frac{-T_{2u+2}}{T_{2u+1}} \right\rfloor + 1$$

Else $s_v = r_\mu, s_{v+1} = 0, P_v = p_\mu, P_{v+1} = p_{\mu+1}$.

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Notice that S and g_S are disjoint sets (otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

(Bresinsky, 1979) Monomial curves
(Kunz, 1979, Herzog, 1970) Gorestein rings
(Apéry, 1945) Classification plane of algebraic branches
(Buchweitz, 1981) Weierstrass semigroups
(Pellikaan and Torres, 1999) Algebraic codes

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Notice that S and g_S are disjoint sets (otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

(Bresinsky, 1979) Monomial curves
(Kunz, 1979, Herzog, 1970) Gorestein rings
(Apéry, 1945) Classification plane of algebraic branches
(Buchweitz, 1981) Weierstrass semigroups
(Pellikaan and Torres, 1999) Algebraic codes

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Notice that S and g_S are disjoint sets (otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

(Bresinsky, 1979) Monomial curves
(Kunz, 1979, Herzog, 1970) Gorestein rings
(Apéry, 1945) Classification plane of algebraic branches
(Buchweitz, 1981) Weierstrass semigroups
(Pellikaan and Torres, 1999) Algebraic codes

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Notice that S and g_S are disjoint sets (otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

(Bresinsky, 1979) Monomial curves
(Kunz, 1979, Herzog, 1970) Gorestein rings
(Apéry, 1945) Classification plane of algebraic branches
(Buchweitz, 1981) Weierstrass semigroups
(Pellikaan and Torres, 1999) Algebraic codes

Theorem (Sylvester) Semigroup $\langle p, q\rangle$ is always symmetric.

Theorem (R.A. and Rødseth 2009)
Let $S = \langle a, a+d, \ldots, a+kd, c\rangle$ with $\gcd(a,d) = 1$. Then, S is symmetric if and only if one of the following conditions is satisfied.

(i) $s_v = 1$,

(ii) $s_v \equiv 2 \pmod{k}$ and $s_{v+1} = 0$,

(iii) $s_v \equiv 2 \pmod{k}$ and $s_v = a$,

(iv) $s_v - s_{v+1} = 1$ and $R_{v+1} = 1 - k$,

(v) $s_v \equiv 2 \pmod{k}$ and $s_v - s_{v+1} > 1$ and $R_{v+1} = 0$,

(vi) $k \geq 2, s_{v+1} = k - 1$ and $R_v = 1$.

Theorem (Sylvester) Semigroup $\langle p, q\rangle$ is always symmetric.

Theorem (R.A. and Rødseth 2009)
Let $S = \langle a, a+d, \ldots, a+kd, c\rangle$ with $\gcd(a,d) = 1$. Then, S is symmetric if and only if one of the following conditions is satisfied.

(i) $s_v = 1$,

(ii) $s_v \equiv 2 \pmod{k}$ and $s_{v+1} = 0$,

(iii) $s_v \equiv 2 \pmod{k}$ and $s_v = a$,

(iv) $s_v - s_{v+1} = 1$ and $R_{v+1} = 1 - k$,

(v) $s_v \equiv 2 \pmod{k}$ and $s_v - s_{v+1} > 1$ and $R_{v+1} = 0$,

(vi) $k \geq 2, s_{v+1} = k - 1$ and $R_v = 1$.

Let $N(S)$ be the number of gaps in S.

Theorem (Selmer) $N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1)$.

A semigroup S is symmetric if and only if $g(S) + 1 = 2N(S)$.

Lemma (Folklore) S is symmetric if and only if there is an i_0 such that

$$w(i_0) - w(i) = w(i_0 - i) \text{ for all } i$$

where $w(i)$ denote the unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod{m}$.

Remark If the above holds for some (fixed) i_0 and all i then $w(i_0) = \max Ap(S; m)$.

Let $N(S)$ be the number of gaps in S.

Theorem (Selmer) $N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1)$.

A semigroup S is symmetric if and only if $g(S) + 1 = 2N(S)$.

Lemma (Folklore) S is symmetric if and only if there is an i_0 such that

$$w(i_0) - w(i) = w(i_0 - i) \text{ for all } i$$

where $w(i)$ denote the unique $w \in Ap(S;m)$ satisfying $w \equiv i \pmod{m}$.

Remark If the above holds for some (fixed) i_0 and all i then $w(i_0) = \max Ap(S;m)$.

Let $N(S)$ be the number of gaps in S.

Theorem (Selmer) $N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1)$.

A semigroup S is symmetric if and only if $g(S) + 1 = 2N(S)$.

Lemma (Folklore) S is symmetric if and only if there is an i_0 such that

$$w(i_0) - w(i) = w(i_0 - i) \text{ for all } i$$

where $w(i)$ denote the unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod{m}$.

Remark If the above holds for some (fixed) i_0 and all i then $w(i_0) = \max Ap(S; m)$.

Let $N(S)$ be the number of gaps in S.

Theorem (Selmer) $N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1)$.

A semigroup S is symmetric if and only if $g(S) + 1 = 2N(S)$.
Lemma (Folklore) S is symmetric if and only if there is an i_0 such that

$$w(i_0) - w(i) = w(i_0 - i) \text{ for all } i$$

where $w(i)$ denote the unique $w \in Ap(S;m)$ satisfying $w \equiv i \pmod{m}$.

Remark If the above holds for some (fixed) i_0 and all i then $w(i_0) = \max Ap(S;m)$.

Let $N(S)$ be the number of gaps in S.

Theorem (Selmer) $N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1)$.

A semigroup S is symmetric if and only if $g(S) + 1 = 2N(S)$.
Lemma (Folklore) S is symmetric if and only if there is an i_0 such that

$$w(i_0) - w(i) = w(i_0 - i) \text{ for all } i$$

where $w(i)$ denote the unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod{m}$.

Remark If the above holds for some (fixed) i_0 and all i then $w(i_0) = \max Ap(S; m)$.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c \rangle$.

Let $S = \langle a_1, \ldots, a_n \rangle$ and let $d_i = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1/\prod_{j\neq 1} d_j, \ldots, a_n/\prod_{j\neq n} d_j\}$.

Corollary (Frőberg, Gottlieb and Hăggkvist 1987) $\langle a_1, a_2, a_3 \rangle$ is symmetric if and only if its derived is generated by two elements.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c \rangle$.

Let $S = \langle a_1, \ldots, a_n \rangle$ and let $d_i = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1 / \prod_{j \neq 1} d_j, \ldots, a_n / \prod_{j \neq n} d_j\}$.

Corollary (Frőberg, Gottlieb and Hăggkvist 1987) $\langle a_1, a_2, a_3 \rangle$ is symmetric if and only if its derived is generated by two elements.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c\rangle$.

Let $S = \langle a_1, \ldots, a_n\rangle$ and let $d_i = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1/\prod_{j\neq 1} d_j, \ldots, a_n/\prod_{j\neq n} d_j\}$.

Corollary (Frőberg, Gottlieb and Hăggkvist 1987) $\langle a_1, a_2, a_3\rangle$ is symmetric if and only if its derived is generated by two elements.

A semigroup S is pseudo-symmetric if and only if

$$g(S) = 2N(S) - 2.$$

If S is pseudo-symmetric then $S \cup g_S = \mathbb{Z} \setminus \{g/2\}$.

Lemma

$$w(g/2+i) + w(g/2-i) = w(g) + \begin{cases} m & \text{if } i \equiv 0 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases}$$

where $w(i)$ denote the unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod{m}$.

A semigroup S is pseudo-symmetric if and only if

$$g(S) = 2N(S) - 2.$$

If S is pseudo-symmetric then $S \cup g_S = \mathbb{Z} \setminus \{g/2\}$.

Lemma

$$w(g/2+i) + w(g/2-i) = w(g) + \begin{cases} m & \text{if } i \equiv 0 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases}$$

where $w(i)$ denote the unique $w \in Ap(S;m)$ satisfying $w \equiv i \pmod{m}$.

A semigroup S is pseudo-symmetric if and only if

$$g(S) = 2N(S) - 2.$$

If S is pseudo-symmetric then $S \cup g_S = \mathbb{Z} \setminus \{g/2\}$.

Lemma

$$w(g/2+i) + w(g/2-i) = w(g) + \begin{cases} m & \text{if } i \equiv 0 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases}$$

where $w(i)$ denote the unique $w \in Ap(S;m)$ satisfying $w \equiv i \pmod{m}$.