Le problème diophantien de Frobenius : algorithmes et génŕalisations

J.L. Ramírez Alfonsín

I3M, Université Montpellier 2

Problème diophantien de Frobenius

Soient $a_1, \ldots, a_n$ de entiers positifs avec $\gcd(a_1, \ldots, a_n) = 1$, trouver le plus grand entier (appelé le nombre de Frobenius et désigné par $g(a_1, \ldots, a_n)$) qui n'est pas representable comme une combinaison linéaire de $a_1, \ldots, a_n$ à coefficients non négatifs.

Exemple : $a_1 = 3$, $a_2 = 8$

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

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

On désigne $\langle a_1, \ldots, a_n \rangle$ le semigroupe numérique engendré par $a_1, \ldots, a_n$.

Problème diophantien de Frobenius

Soient $a_1, \ldots, a_n$ de entiers positifs avec $\gcd(a_1, \ldots, a_n) = 1$, trouver le plus grand entier (appelé le nombre de Frobenius et désigné par $g(a_1, \ldots, a_n)$) qui n'est pas representable comme une combinaison linéaire de $a_1, \ldots, a_n$ à coefficients non négatifs.

Exemple : $a_1 = 3$, $a_2 = 8$

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

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

On désigne $\langle a_1, \ldots, a_n \rangle$ le semigroupe numérique engendré par $a_1, \ldots, a_n$.

Problème diophantien de Frobenius

Soient $a_1, \ldots, a_n$ de entiers positifs avec $\gcd(a_1, \ldots, a_n) = 1$, trouver le plus grand entier (appelé le nombre de Frobenius et désigné par $g(a_1, \ldots, a_n)$) qui n'est pas representable comme une combinaison linéaire de $a_1, \ldots, a_n$ à coefficients non négatifs.

Exemple : $a_1 = 3$, $a_2 = 8$

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

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

On désigne $\langle a_1, \ldots, a_n \rangle$ le semigroupe numérique engendré par $a_1, \ldots, a_n$.

Problème diophantien de Frobenius

Soient $a_1, \ldots, a_n$ de entiers positifs avec $\gcd(a_1, \ldots, a_n) = 1$, trouver le plus grand entier (appelé le nombre de Frobenius et désigné par $g(a_1, \ldots, a_n)$) qui n'est pas representable comme une combinaison linéaire de $a_1, \ldots, a_n$ à coefficients non négatifs.

Exemple : $a_1 = 3$, $a_2 = 8$

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

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

On désigne $\langle a_1, \ldots, a_n \rangle$ le semigroupe numérique engendré par $a_1, \ldots, a_n$.

Problème diophantien de Frobenius

Soient $a_1, \ldots, a_n$ de entiers positifs avec $\gcd(a_1, \ldots, a_n) = 1$, trouver le plus grand entier (appelé le nombre de Frobenius et désigné par $g(a_1, \ldots, a_n)$) qui n'est pas representable comme une combinaison linéaire de $a_1, \ldots, a_n$ à coefficients non négatifs.

Exemple : $a_1 = 3$, $a_2 = 8$

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

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

On désigne $\langle a_1, \ldots, a_n \rangle$ le semigroupe numérique engendré par $a_1, \ldots, a_n$.

Problème diophantien de Frobenius

Soient $a_1, \ldots, a_n$ de entiers positifs avec $\gcd(a_1, \ldots, a_n) = 1$, trouver le plus grand entier (appelé le nombre de Frobenius et désigné par $g(a_1, \ldots, a_n)$) qui n'est pas representable comme une combinaison linéaire de $a_1, \ldots, a_n$ à coefficients non négatifs.

Exemple : $a_1 = 3$, $a_2 = 8$

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

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

On désigne $\langle a_1, \ldots, a_n \rangle$ le semigroupe numérique engendré par $a_1, \ldots, a_n$.

Théorème $g(a_1, \ldots, a_n)$ existe et il est fini.

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then $m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let P and $-Q$ be the sum of positive and negative terms respectively (and so $P - Q = 1$).

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 < k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

Théorème $g(a_1, \ldots, a_n)$ existe et il est fini.

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then
$m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let P and $-Q$ be the sum of positive and negative terms respectively (and so $P - Q = 1$).

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 < k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

Théorème $g(a_1, \ldots, a_n)$ existe et il est fini.

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then
$m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let P and $-Q$ be the sum of positive and negative terms respectively (and so $P - Q = 1$).

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 < k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

Théorème $g(a_1, \ldots, a_n)$ existe et il est fini.

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then
$m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let P and $-Q$ be the sum of positive and negative terms respectively (and so $P - Q = 1$).

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 < k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

Théorème $g(a_1, \ldots, a_n)$ existe et il est fini.

Proof (sketch). Since $\gcd(a_1, \ldots, a_n) = 1$ then
$m_1 a_1 + \cdots + m_n a_n = 1$ for some $m_i \in \mathbb{N}$

Let P and $-Q$ be the sum of positive and negative terms respectively (and so $P - Q = 1$).

Let $k \geq 0$ then $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'$ with $h \geq 0$ and $0 < k' < a_1$

So, $(a_1 - 1)Q + k = ha_1 + (a_1 - 1 - k')Q + k'P$.

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

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

Méthods

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

Théorème (R.A., 1996) Calculer $g(a_1, \ldots, a_n)$ est $\mathcal{NP}$-difficile.

Quand $n = 3$

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

Quand $n \geq 4$

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

Méthods

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

Théorème (R.A., 1996) Calculer $g(a_1, \ldots, a_n)$ est $\mathcal{NP}$-difficile.

Quand $n = 3$

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

Quand $n \geq 4$

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

Méthods

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

Théorème (R.A., 1996) Calculer $g(a_1, \ldots, a_n)$ est $\mathcal{NP}$-difficile.

Quand $n = 3$

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

Quand $n \geq 4$

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

Méthods

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

Théorème (R.A., 1996) Calculer $g(a_1, \ldots, a_n)$ est $\mathcal{NP}$-difficile.

Quand $n = 3$

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

Quand $n \geq 4$

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

Méthode de Kannan

Théorème (Kannan, 1992) Il existe un algorithme polynomial qui détermine $g(a_1, \ldots, a_n)$ quand $n \geq 2$ est fixé.

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

The least positive real t so that $tP + L$ equals $\mathbb{R}^n$ is called the covering radius of P with respect to L (denoted by $\mu(P, L)$).

Méthode de Kannan

Théorème (Kannan, 1992) Il existe un algorithme polynomial qui détermine $g(a_1, \ldots, a_n)$ quand $n \geq 2$ est fixé.

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

The least positive real t so that $tP + L$ equals $\mathbb{R}^n$ is called the covering radius of P with respect to L (denoted by $\mu(P, L)$).

Méthode de Kannan

Théorème (Kannan, 1992) Il existe un algorithme polynomial qui détermine $g(a_1, \ldots, a_n)$ quand $n \geq 2$ est fixé.

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

The least positive real t so that $tP + L$ equals $\mathbb{R}^n$ is called the covering radius of P with respect to L (denoted by $\mu(P, L)$).

Méthode de Kannan

Théorème (Kannan, 1992) Il existe un algorithme polynomial qui détermine $g(a_1, \ldots, a_n)$ quand $n \geq 2$ est fixé.

Let P be a closed bounded convex set in $\mathbb{R}^n$ and let L be a lattice of dimension n also in $\mathbb{R}^n$.

The least positive real t so that $tP + L$ equals $\mathbb{R}^n$ is called the covering radius of P with respect to L (denoted by $\mu(P, L)$).

Théorème (Kannan, 1992) Let

$$L = \{(x_1, \ldots, x_{n-1}) | x_i \text{ integers and } \sum_{i=1}^{n-1} a_i x_i \equiv 0 \bmod a_n\}$$

and

$$S = \{(x_1, \ldots, x_{n-1}) | x_i \geq 0 \text{ reals and } \sum_{i=1}^{n-1} a_i x_i \leq 1\}.$$

Then, $\mu(S, L) = g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$

Théorème (Kannan, 1992) Let

$$L = \{(x_1, \ldots, x_{n-1}) | x_i \text{ integers and } \sum_{i=1}^{n-1} a_i x_i \equiv 0 \bmod a_n\}$$

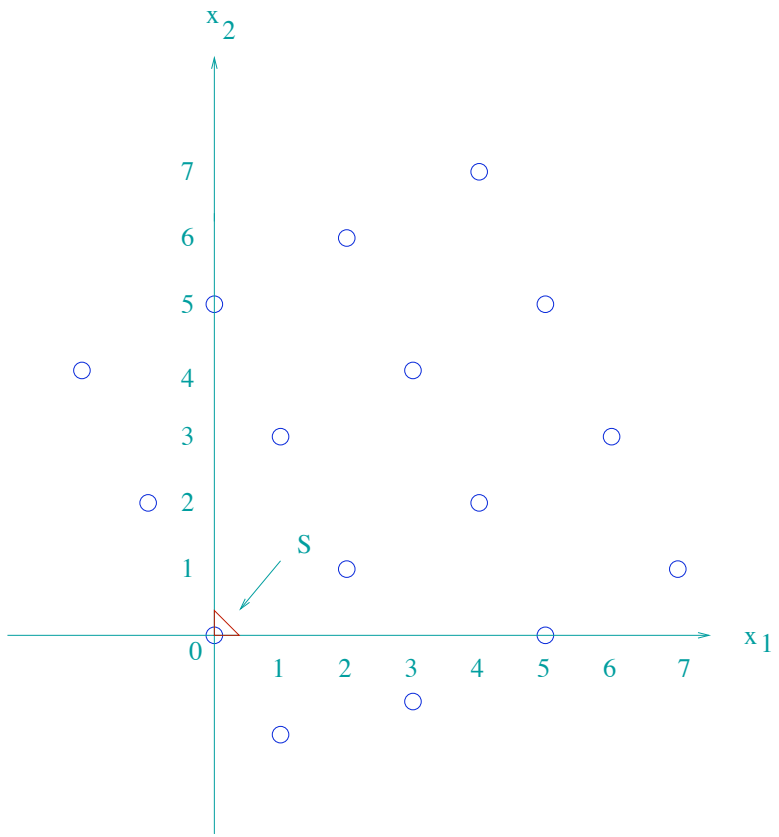
and

$$S = \{(x_1, \ldots, x_{n-1}) | x_i \geq 0 \text{ reals and } \sum_{i=1}^{n-1} a_i x_i \leq 1\}.$$

Then, $\mu(S, L) = g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$

Example 1 : Let $a_1 = 3, a_2 = 4$ and $a_3 = 5$.

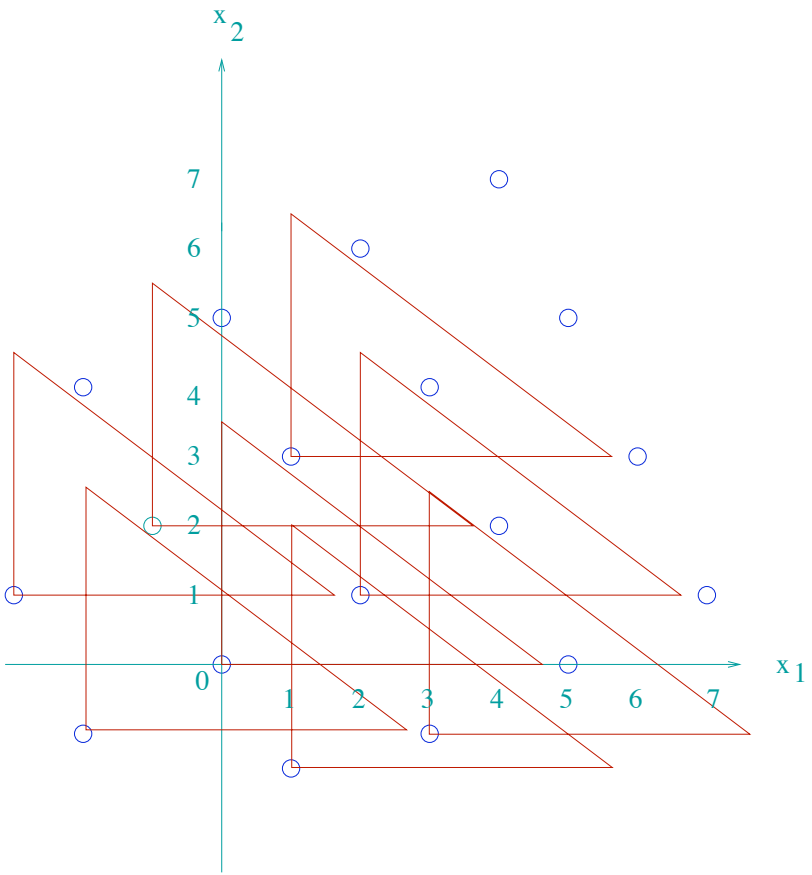
Example 1 : Let $a_1 = 3, a_2 = 4$ and $a_3 = 5$.

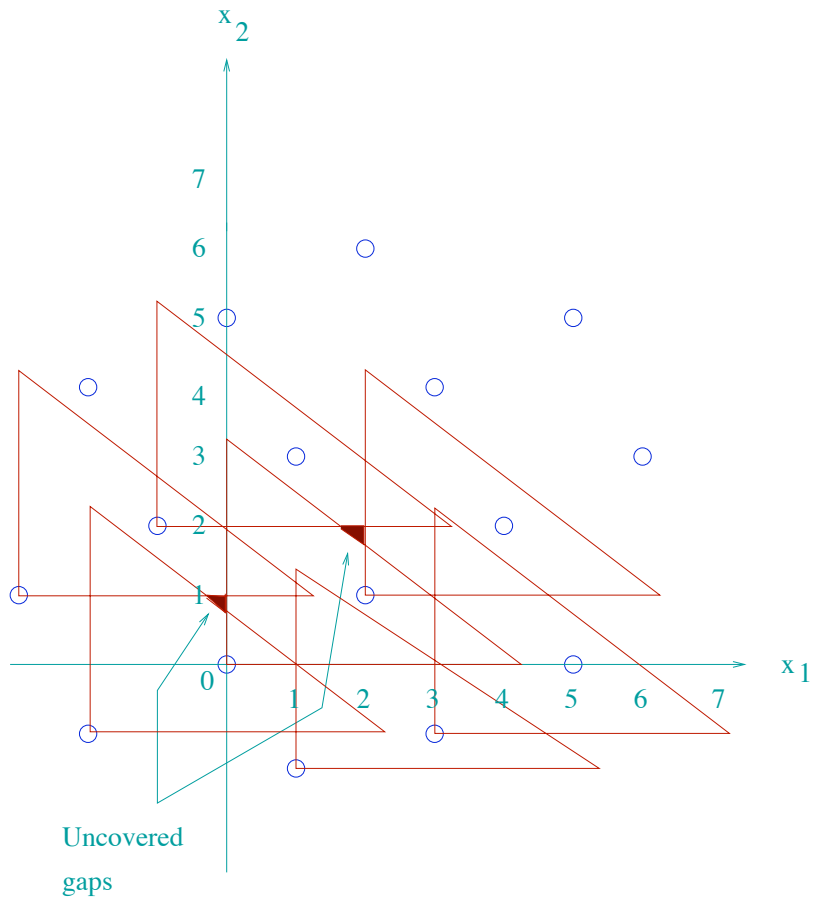


Example 1 cont ... then, $g(3,4,5) = 2$ and thus $\mu(L,S) = 14$

Notice that $(14)S$ covers the plane while $(13)S$ does not.

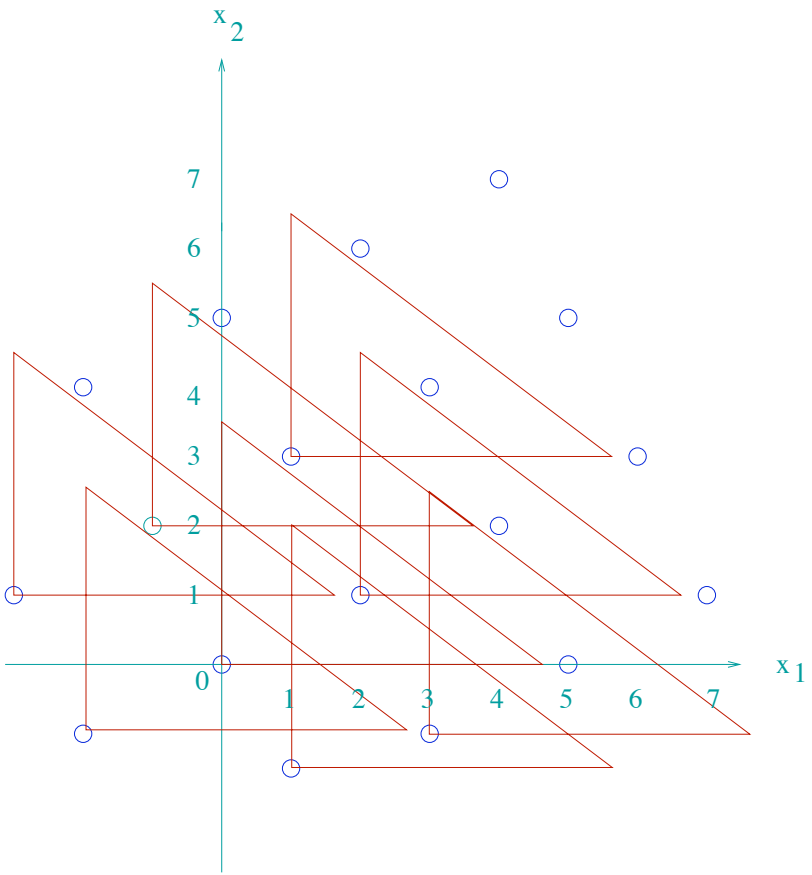
Example 1 cont ... then, $g(3,4,5) = 2$ and thus $\mu(L,S) = 14$

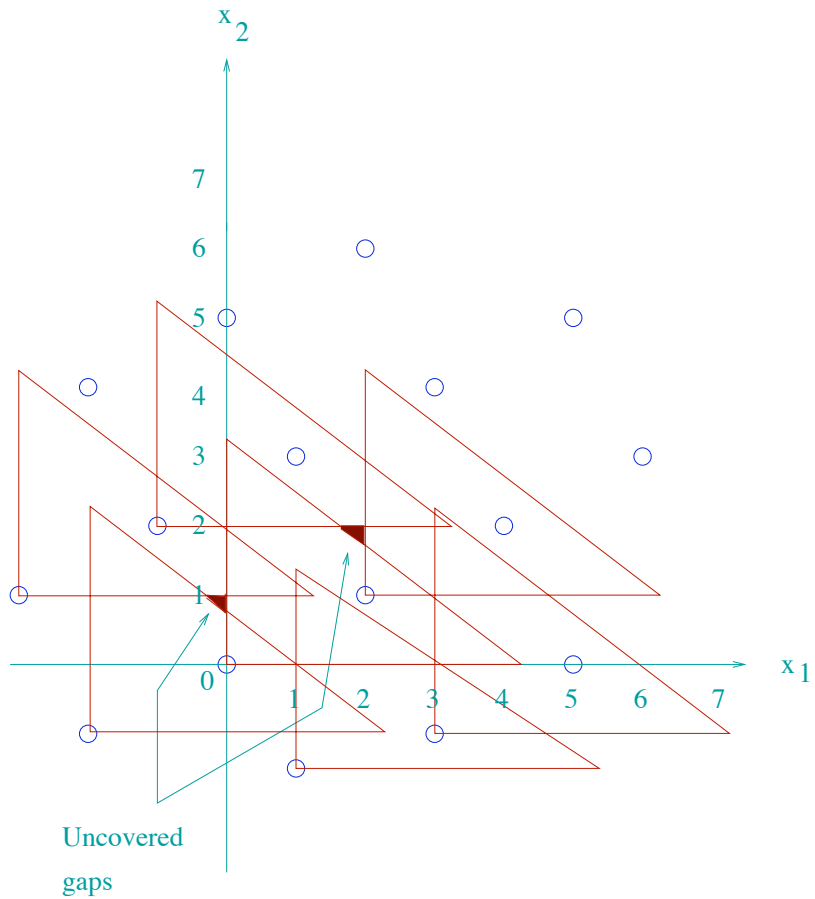




Notice that $(14)S$ covers the plane while $(13)S$ does not.

Example 1 cont ... then, $g(3,4,5) = 2$ and thus $\mu(L,S) = 14$

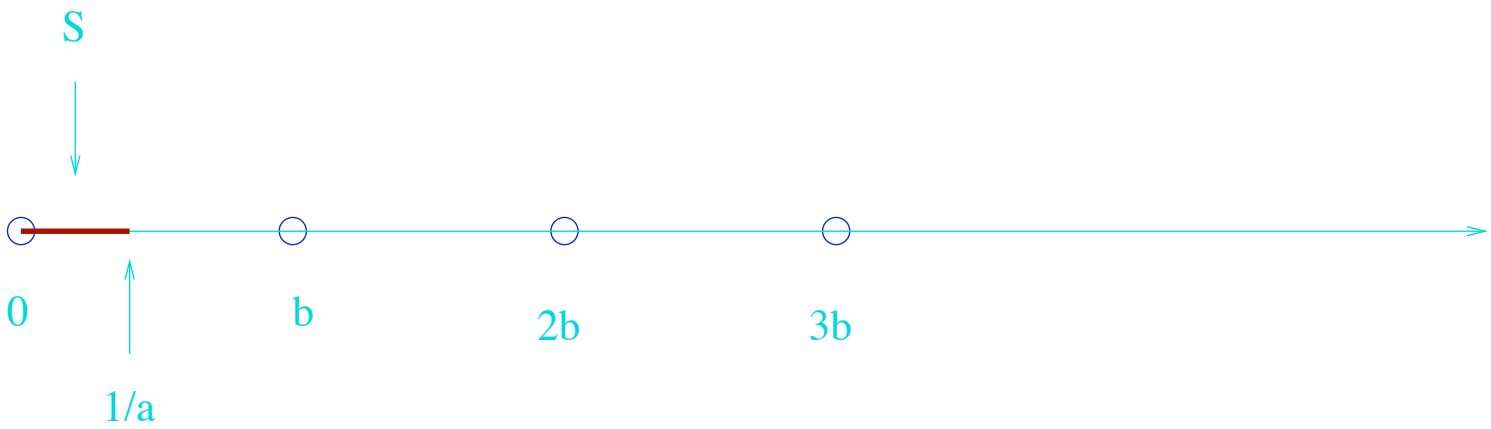




Notice that $(14)S$ covers the plane while $(13)S$ does not.

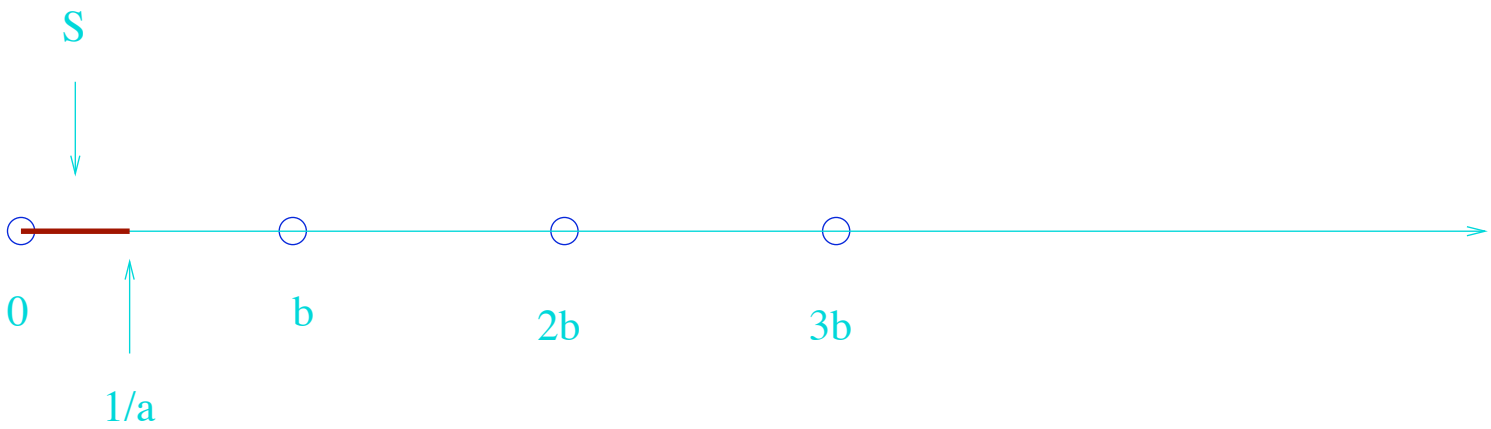
Example 2 : Let a, b be positive integers with $\gcd(a, b) = 1$.
Minimum integer t such that tS covers the interval $[0, b]$ is ab.
Thus, $g(a, b) = \mu(S, L) - a - b = ab - a - b$.

Example 2 : Let a, b be positive integers with $\gcd(a, b) = 1$.



Minimum integer t such that tS covers the interval $[0, b]$ is ab.
Thus, $g(a, b) = \mu(S, L) - a - b = ab - a - b$.

Example 2 : Let a, b be positive integers with $\gcd(a, b) = 1$.



Minimum integer t such that tS covers the interval $[0, b]$ is ab.
Thus, $g(a, b) = \mu(S, L) - a - b = ab - a - b$.

Heap and Lynn's method

Let $B = (b_{i,j})$, $1 \leq, i, j \leq n$ be a positive matrix, that is, $b_{i,j} \geq 0$.

B reducible if there exists an $(n \times n)$ permutation matrix P such that

$$PBP^T = \begin{bmatrix} B_{1,1} & B_{1,2} \\ 0 & B_{2,2} \end{bmatrix}$$

Heap and Lynn's method

Let $B = (b_{i,j})$, $1 \leq, i, j \leq n$ be a positive matrix, that is, $b_{i,j} \geq 0$.

B reducible if there exists an $(n \times n)$ permutation matrix P such that

$$PBP^T = \begin{bmatrix} B_{1,1} & B_{1,2} \\ 0 & B_{2,2} \end{bmatrix}$$

Heap and Lynn's method

Let $B = (b_{i,j})$, $1 \leq, i, j \leq n$ be a positive matrix, that is, $b_{i,j} \geq 0$.

B reducible if there exists an $(n \times n)$ permutation matrix P such that

$$PBP^T = \begin{bmatrix} B_{1,1} & B_{1,2} \\ 0 & B_{2,2} \end{bmatrix}$$

Let B be a real $(m \times m)$-matrix. Let $G(B)$ be the directed graph with $V(G) = \{1, \ldots, m\}$ and directed edge form i to j if and only if $b_{i,j} \neq 0$.

Theorem B irreducible if and only if $G(B)$ is strongly connected.

An irreducible nonnegative matrix B is primitive if $B^t > 0$ for some integer $t \geq 1$. The least integer $\gamma(B)$ such that $B^{\gamma(B)} > 0$ is called the index of primitivity of B.

Let B be a real $(m \times m)$-matrix. Let $G(B)$ be the directed graph with $V(G) = \{1, \ldots, m\}$ and directed edge form i to j if and only if $b_{i,j} \neq 0$.

Theorem B irreducible if and only if $G(B)$ is strongly connected.

An irreducible nonnegative matrix B is primitive if $B^t > 0$ for some integer $t \geq 1$. The least integer $\gamma(B)$ such that $B^{\gamma(B)} > 0$ is called the index of primitivity of B.

Let B be a real $(m \times m)$-matrix. Let $G(B)$ be the directed graph with $V(G) = \{1, \ldots, m\}$ and directed edge form i to j if and only if $b_{i,j} \neq 0$.

Theorem B irreducible if and only if $G(B)$ is strongly connected.

An irreducible nonnegative matrix B is primitive if $B^t > 0$ for some integer $t \geq 1$. The least integer $\gamma(B)$ such that $B^{\gamma(B)} > 0$ is called the index of primitivity of B.

Lemma 1 (Heap and Lynn, 1964) Let B be a primitive matrix and let $0 < a_1 < \cdots < a_k$ be the distinct lengths of all *elementary* circuits of $G(B)$. Then, $\gcd(a_1, \ldots, a_n) = 1$ and the length L, of any circuit of $G(B)$ can be expressed in the form $L = \sum_{i=1}^{n} x_i a_i$ with $x_i \geq 0$ for all i.

Lemma 2 (Heap and Lynn, 1964) If B is primitive then $\gamma(B)$ is the least integer such that for all $m \geq \gamma(B)$ there is a path of lenght m connecting two arbitrary (not necessarily distinct) vertices of $G(B)$.

Lemma 1 (Heap and Lynn, 1964) Let B be a primitive matrix and let $0 < a_1 < \cdots < a_k$ be the distinct lengths of all *elementary* circuits of $G(B)$. Then, $\gcd(a_1, \ldots, a_n) = 1$ and the length L, of any circuit of $G(B)$ can be expressed in the form $L = \sum_{i=1}^{n} x_i a_i$ with $x_i \geq 0$ for all i.

Lemma 2 (Heap and Lynn, 1964) If B is primitive then $\gamma(B)$ is the least integer such that for all $m \geq \gamma(B)$ there is a path of lenght m connecting two arbitrary (not necessarily distinct) vertices of $G(B)$.

Lemma 3 (Heap and Lynn, 1964) Let B be a primitive matrix and let $0 < a_1 < \cdots < a_k$ be the distinct lengths of all elementary circuits of $G(B)$. Then, $g(a_1, \ldots, a_n) \leq \gamma(B) - 1$.

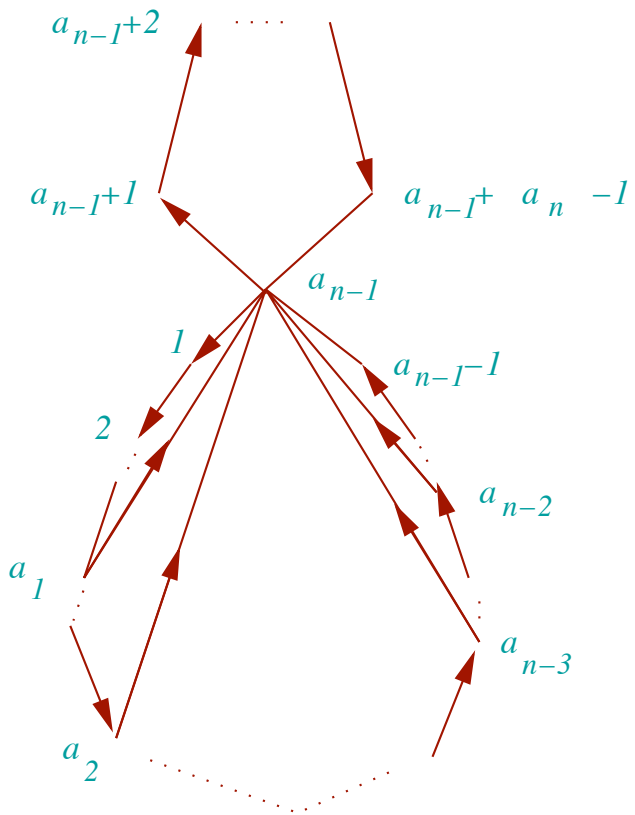
Let $B' = (b'_{i,j})$, $1 \leq, i, j \leq s = a_n + a_{n-1} - 1$ be the matrix defined by

$$b'_{i,j} = \begin{cases} 1 & \text{if } j = i+1 \text{ with } i = 1, \ldots, s-1 \text{ and } i \neq a_{n-1}, \\ 1 & \text{if } j = 1 \text{ with } i = s \text{ or } a_t,\ t = 1, \ldots, n-1, \\ 1 & \text{if } i = 1 \text{ and } j = a_{n-1} + 1, \\ 0 & \text{otherwise.} \end{cases}$$

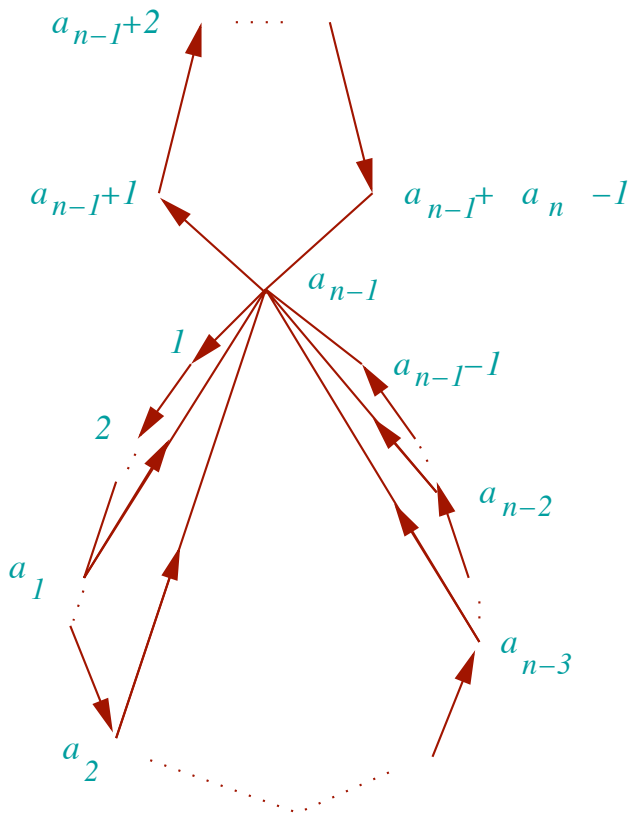
Lemma 3 (Heap and Lynn, 1964) Let B be a primitive matrix and let $0 < a_1 < \cdots < a_k$ be the distinct lengths of all elementary circuits of $G(B)$. Then, $g(a_1, \ldots, a_n) \leq \gamma(B) - 1$.

Let $B' = (b'_{i,j})$, $1 \leq, i, j \leq s = a_n + a_{n-1} - 1$ be the matrix defined by

$$b'_{i,j} = \begin{cases} 1 & \text{if } j = i + 1 \text{ with } i = 1, \ldots, s-1 \text{ and } i \neq a_{n-1}, \\ 1 & \text{if } j = 1 \text{ with } i = s \text{ or } a_t,\ t = 1, \ldots, n-1, \\ 1 & \text{if } i = 1 \text{ and } j = a_{n-1} + 1, \\ 0 & \text{otherwise.} \end{cases}$$



Theorem (Heap and Lynn, 1964) $g(a_1, \ldots, a_n) = \gamma(B') - 2a_n + 1$.



Theorem (Heap and Lynn, 1964) $g(a_1, \ldots, a_n) = \gamma(B') - 2a_n + 1$.

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

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

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

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

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

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

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

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

$Ap(S; m)$ consititutes a complete set of residues $\pmod m$ (there is a unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod m$.

$$g(a_1, \ldots, a_n) = \max Ap(S; m) - m.$$

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

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

$Ap(S; m)$ consititutes a complete set of residues $\pmod m$ (there is a unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod m$.

$$g(a_1, \ldots, a_n) = \max Ap(S; m) - m.$$

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

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

$Ap(S; m)$ consititutes a complete set of residues $\pmod m$ (there is a unique $w \in Ap(S; m)$ satisfying $w \equiv i \pmod m$.

$$g(a_1, \ldots, a_n) = \max Ap(S; m) - m.$$

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

$$H(A[S],z) = \sum_{i \in S} z^s = \sum_{w \in Ap(S;m)} \sum_{i=0}^{\infty} z^{w+mi}$$

$$= \sum_{w \in Ap(S;m)} z^w \sum_{i=0}^{\infty} z^w$$

$$\text{So, } H(A[S],z) = \frac{1}{1-x^m} \sum_{w \in Ap(S;m)} z^w.$$

$$\text{Hence, } deg(H(A[S],z)) = \max Ap(S;m) - m = g(a_1,\ldots,a_n).$$

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

$$H(A[S],z) = \sum_{i \in S} z^s = \sum_{w \in Ap(S;m)} \sum_{i=0}^{\infty} z^{w+mi}$$

$$= \sum_{w \in Ap(S;m)} z^w \sum_{i=0}^{\infty} z^w$$

So, $H(A[S],z) = \dfrac{1}{1-x^m} \displaystyle\sum_{w \in Ap(S;m)} z^w.$

Hence, $deg(H(A[S],z)) = \max Ap(S;m) - m = g(a_1,\ldots,a_n).$

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

$$H(A[S],z) = \sum_{i \in S} z^s = \sum_{w \in Ap(S;m)} \sum_{i=0}^{\infty} z^{w+mi}$$

$$= \sum_{w \in Ap(S;m)} z^w \sum_{i=0}^{\infty} z^w$$

$$\text{So, } H(A[S],z) = \frac{1}{1-x^m} \sum_{w \in Ap(S;m)} z^w.$$

Hence, $deg(H(A[S],z)) = \max Ap(S;m) - m = g(a_1,\ldots,a_n)$.

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

$$H(A[S],z) = \sum_{i \in S} z^s = \sum_{w \in Ap(S;m)} \sum_{i=0}^{\infty} z^{w+mi}$$

$$= \sum_{w \in Ap(S;m)} z^w \sum_{i=0}^{\infty} z^w$$

$$\text{So, } H(A[S],z) = \frac{1}{1-x^m} \sum_{w \in Ap(S;m)} z^w.$$

$$\text{Hence, } deg(H(A[S],z)) = \max Ap(S;m) - m = g(a_1,\ldots,a_n).$$

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

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 $s_v, s_{v+1}, P_v, P_{v+1}$ are some *particular* integers.

Remark : Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

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

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 $s_v, s_{v+1}, P_v, P_{v+1}$ are some *particular* integers.

Remark : Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

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

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 $s_v, s_{v+1}, P_v, P_{v+1}$ are some *particular* integers.

Remark : Contains the case $n = 3$ when $k = 1$ and $b = a + d$.

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

La méthode de Scarf et Shallcross

Un corps représenté par $\{x \in \mathbb{R}^{n-1} : Ax \leq b\}$ avec $b \in \mathbb{Z}^n$ et A une $(n \times n-1)$-matrice réelle est un corps maximal sans points entiers si elle ne contient pas un point à coordonnées entières à son intéruieur et si n'importe quelle corps strictement plus grand obtenu en relaxant l'une des inégalités contient un point entier à son intérieur.

Soit A une $(n \times n-1)$-matrice dont ses colonnes engendrent le treillis $(n-1)$-dimensionnel h tel que $a \cdot h = 0$ (c'est-à-dire, les colonnes forment une base de $\{v \in \mathbb{Z}^n : a \cdot v = 0\}$).

$g(a_1, \ldots, a_n) = \max\{a \cdot b | b$ est entier et $\{Ax \leq b\}$ est un corps maximal sans

points entiers$\}$.

La méthode de Scarf et Shallcross

Un corps représenté par $\{x \in \mathbb{R}^{n-1} : Ax \leq b\}$ avec $b \in \mathbb{Z}^n$ et A une $(n \times n-1)$-matrice réelle est un corps maximal sans points entiers si elle ne contient pas un point à coordonnées entières à son intéruieur et si n'importe quelle corps strictement plus grand obtenu en relaxant l'une des inégalités contient un point entier à son intérieur.

Soit A une $(n \times n-1)$-matrice dont ses colonnes engendrent le treillis $(n-1)$-dimensionnel h tel que $a \cdot h = 0$ (c'est-à-dire, les colonnes forment une base de $\{v \in \mathbb{Z}^n : a \cdot v = 0\}$).

$g(a_1, \ldots, a_n) = \max\{a \cdot b | b$ est entier et $\{Ax \leq b\}$ est un corps maximal sans

points entiers$\}$.

La méthode de Scarf et Shallcross

Un corps représenté par $\{x \in \mathbb{R}^{n-1} : Ax \leq b\}$ avec $b \in \mathbb{Z}^n$ et A une $(n \times n-1)$-matrice réelle est un corps maximal sans points entiers si elle ne contient pas un point à coordonnées entières à son intéruieur et si n'importe quelle corps strictement plus grand obtenu en relaxant l'une des inégalités contient un point entier à son intérieur.

Soit A une $(n \times n-1)$-matrice dont ses colonnes engendrent le treillis $(n-1)$-dimensionnel h tel que $a \cdot h = 0$ (c'est-à-dire, les colonnes forment une base de $\{v \in \mathbb{Z}^n : a \cdot v = 0\}$).

$g(a_1, \ldots, a_n) = \max\{a \cdot b | b$ est entier et $\{Ax \leq b\}$ est un corps maximal sans

points entiers$\}$.

Exemple 3 Soient $a_1 = 3$ et $a_2 = 5$ (et donc $n = 2$).

Alors, l'ensemble de vecteurs $h = (h_1, h_2)$ tels que $(3, 5) \cdot (h_1, h_2) = 0$ est donné par $(\pm 5r, \mp 3r)$, $r \geq 0$.

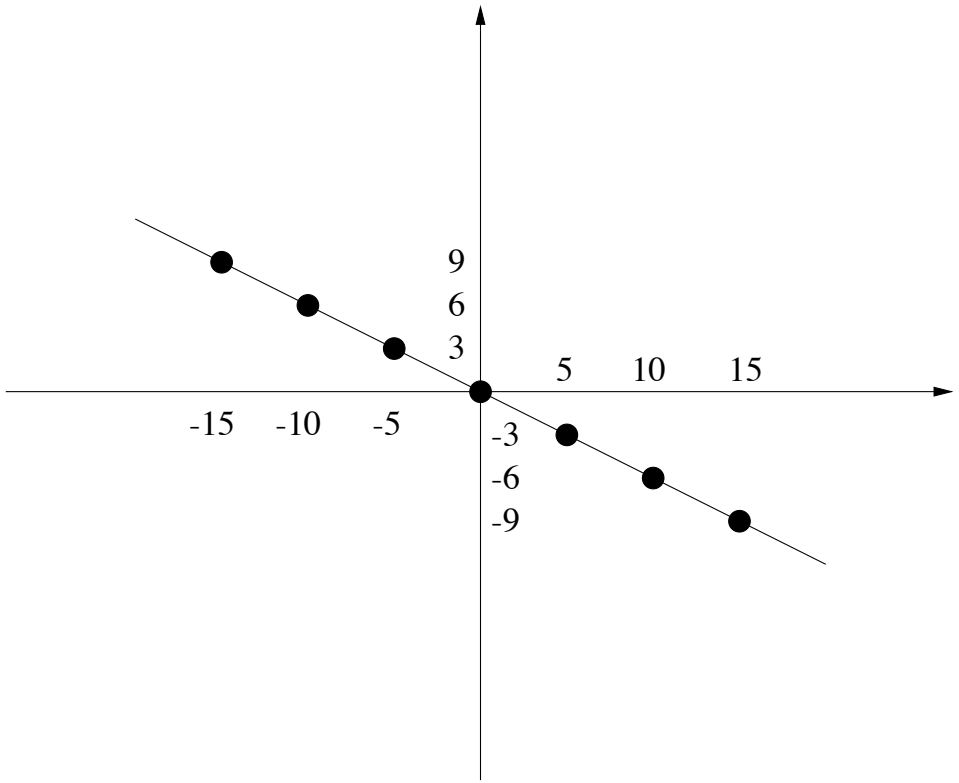
Exemple 3 Soient $a_1 = 3$ et $a_2 = 5$ (et donc $n = 2$).

Alors, l'ensemble de vecteurs $h = (h_1, h_2)$ tels que $(3, 5) \cdot (h_1, h_2) = 0$ est donné par $(\pm 5r, \mp 3r)$, $r \geq 0$.

Exemple 3 Soient $a_1 = 3$ et $a_2 = 5$ (et donc $n = 2$).

Alors, l'ensemble de vecteurs $h = (h_1, h_2)$ tels que $(3, 5) \cdot (h_1, h_2) = 0$ est donné par $(\pm 5r, \mp 3r)$, $r \geq 0$.

Le treillis 1-dimensionnel engendré par h



La matrice $A = \begin{pmatrix} -5 \\ 3 \end{pmatrix}$ engendre le treillis entier h.

On veut donc $b = (b_1, b_2)$ tel que

$$\begin{pmatrix} -5 \\ 3 \end{pmatrix} x \leq \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

soit un treillis libre maximal.

La matrice $A = \begin{pmatrix} -5 \\ 3 \end{pmatrix}$ engendre le treillis entier h.

On veut donc $b = (b_1, b_2)$ tel que

$$\begin{pmatrix} -5 \\ 3 \end{pmatrix} x \leq \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

soit un treillis libre maximal.

On a $-5x \leq b_1$ et $3x \leq b_2$. Donc, $0 < -b_1 < 5$ et $0 < b_2 < 3$ car le corp correspondant doit être une treillis libre maximal.

Alors, $(3,5) \cdot (b_1, b_2)$ est maximal quand $(b_1, b_2) = (-1, 2)$.

On obtient, $g(3,5) = (3,5) \cdot (-1,2) = -3 + 10 = 7$.

On a $-5x \leq b_1$ et $3x \leq b_2$. Donc, $0 < -b_1 < 5$ et $0 < b_2 < 3$ car le corp correspondant doit être une treillis libre maximal.

Alors, $(3,5) \cdot (b_1, b_2)$ est maximal quand $(b_1, b_2) = (-1, 2)$.

On obtient, $g(3,5) = (3,5) \cdot (-1,2) = -3 + 10 = 7$.

On a $-5x \leq b_1$ et $3x \leq b_2$. Donc, $0 < -b_1 < 5$ et $0 < b_2 < 3$ car le corp correspondant doit être une treillis libre maximal.

Alors, $(3,5) \cdot (b_1, b_2)$ est maximal quand $(b_1, b_2) = (-1, 2)$.

On obtient, $g(3,5) = (3,5) \cdot (-1,2) = -3 + 10 = 7$.

Les algorithmes les plus rapides

Einstein, Lichtblau, Strzebonski et Wagon, 2007

Calcule $g(a_1, \ldots, a_4)$ nombres avec 100 chiffres en quelques secondes

Calcule $g(a_1, \ldots, a_{10})$ nombres avec 10 chiffres en deux jours

Roune, 2008

Calcule $g(a_1, \ldots, a_4)$ nombres avec 10 000 chiffres en quelques secondes

Calcule $g(a_1, \ldots, a_{13})$ nombres avec 10 chiffres en quelques jours

Les algorithmes les plus rapides

Einstein, Lichtblau, Strzebonski et Wagon, 2007

Calcule $g(a_1, \ldots, a_4)$ nombres avec 100 chiffres en quelques secondes

Calcule $g(a_1, \ldots, a_{10})$ nombres avec 10 chiffres en deux jours

Roune, 2008

Calcule $g(a_1, \ldots, a_4)$ nombres avec 10 000 chiffres en quelques secondes

Calcule $g(a_1, \ldots, a_{13})$ nombres avec 10 chiffres en quelques jours

Les algorithmes les plus rapides

Einstein, Lichtblau, Strzebonski et Wagon, 2007

Calcule $g(a_1, \ldots, a_4)$ nombres avec 100 chiffres en quelques secondes

Calcule $g(a_1, \ldots, a_{10})$ nombres avec 10 chiffres en deux jours

Roune, 2008

Calcule $g(a_1, \ldots, a_4)$ nombres avec 10 000 chiffres en quelques secondes

Calcule $g(a_1, \ldots, a_{13})$ nombres avec 10 chiffres en quelques jours