Vers une formalisation du L-algorithme en Coq

Motivations

Towards solving the Table Maker's Dilemma on GPU

Pierre Fortin, Mourad Gouicem, Stef Graillat
UPMC Univ Paris 06 and CNRS UMR 7606, LIP6,
4 place Jussieu, F-75252, Paris cedex 05, France
Contact: mourad.gouicem@lip6.fr

***Abstract*—Since 1985, the IEEE 754 standard defines formats, rounding modes and basic operations for floating-point arithmetic. In 2008 the standard has been extended, and recommendations have been added about the rounding of some elementary functions such as trigonometric functions (cosine, sine, tangent and their inverses), exponentials, and logarithms.**

This isolation is efficiently performed using local affine approximations of the targeted function. Stehlé, Lefèvre and Zimmermann extended this method in 2003 [2], [3] (SLZ algorithm) for higher degree approximations, using the Coppersmith method for finding small roots of univariate modular

Plan

Plan

Ce qui a été fait

Plan

Ce qui a été fait

Ce qui reste à faire

Théorèmes des 3 distances

THE THREE GAP THEOREM
(STEINHAUS CONJECTURE)

TONY VAN RAVENSTEIN

(Received 18 November 1986; revised 6 August 1987)

Communicated by J. H. Loxton

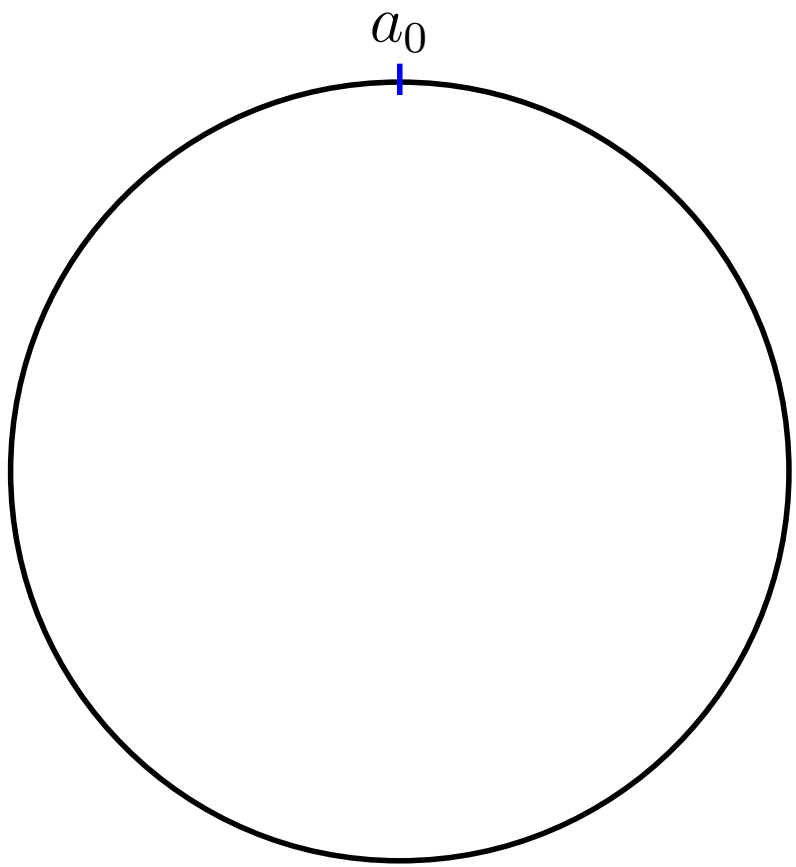
Abstract

This paper is concerned with the distribution of N points placed consecutively around the circle by an angle of α. We offer a new proof of the Steinhaus Conjecture which states that, for

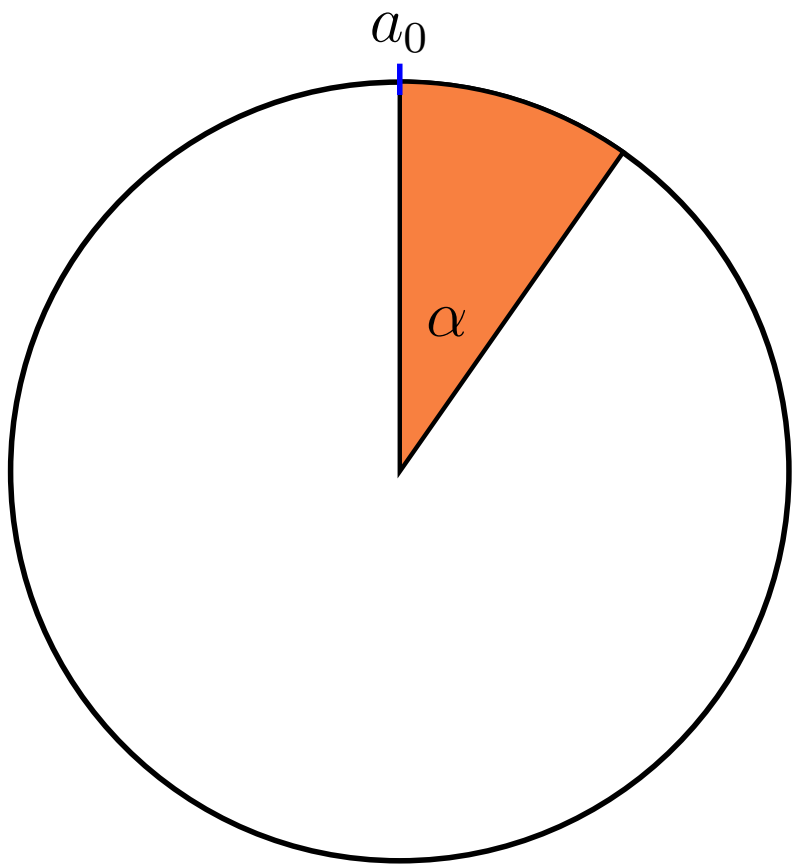
Théorèmes des 3 distances

Théorèmes des 3 distances

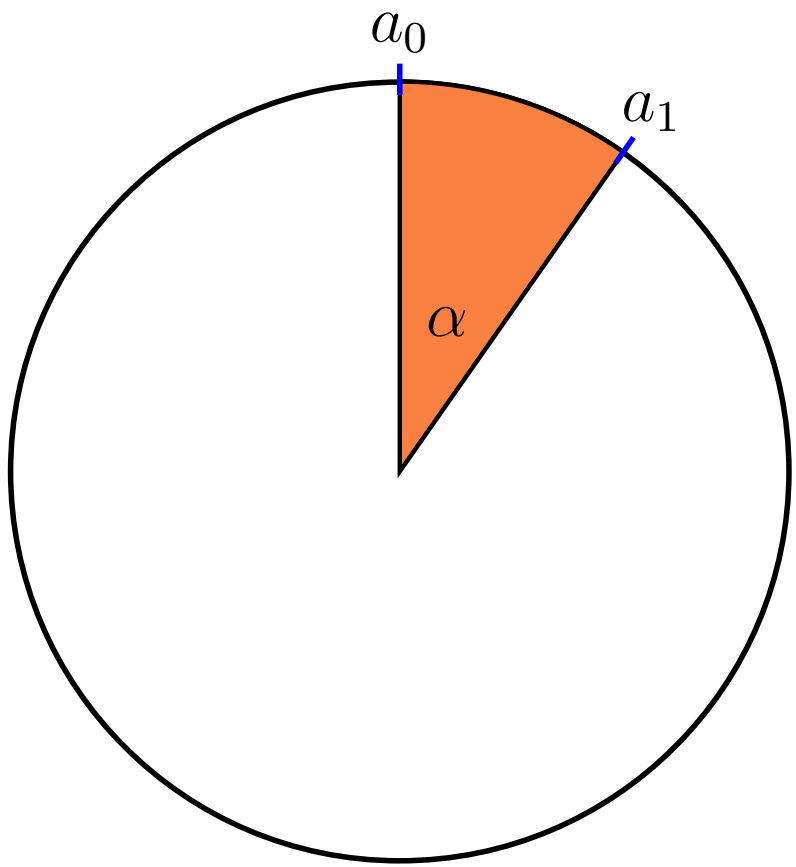
Théorèmes des 3 distances



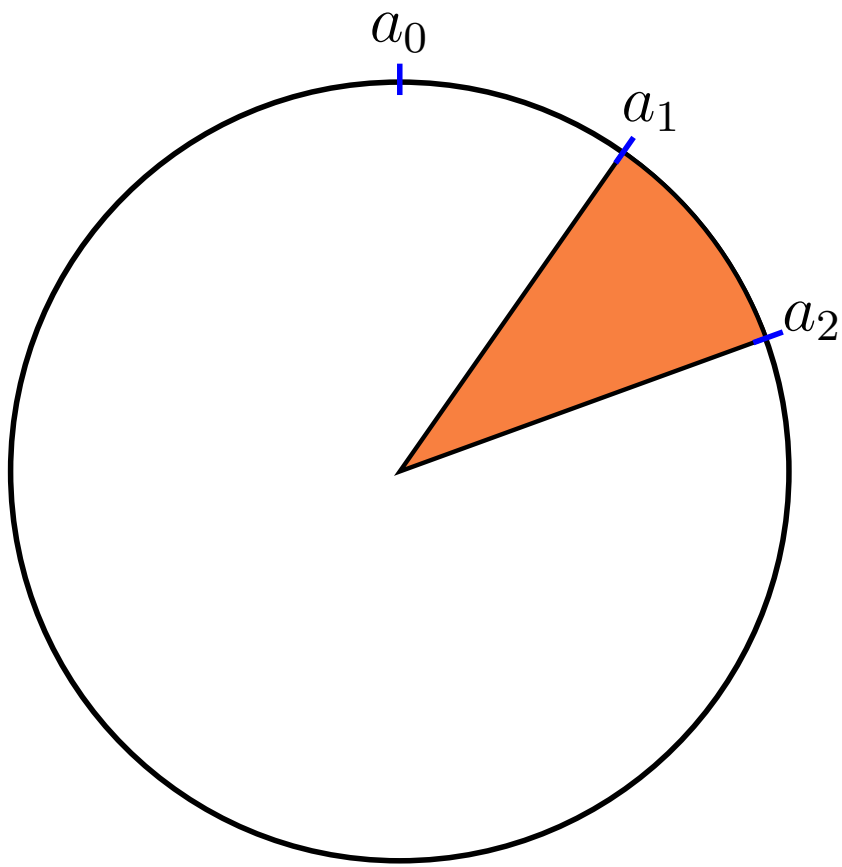
Théorèmes des 3 distances



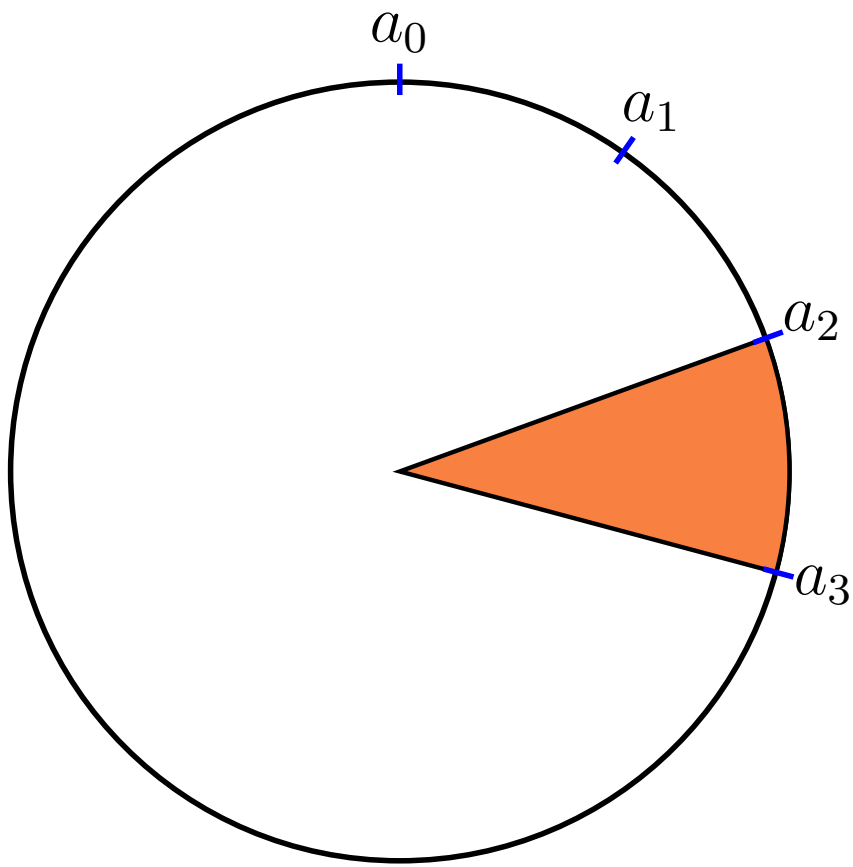
Théorèmes des 3 distances



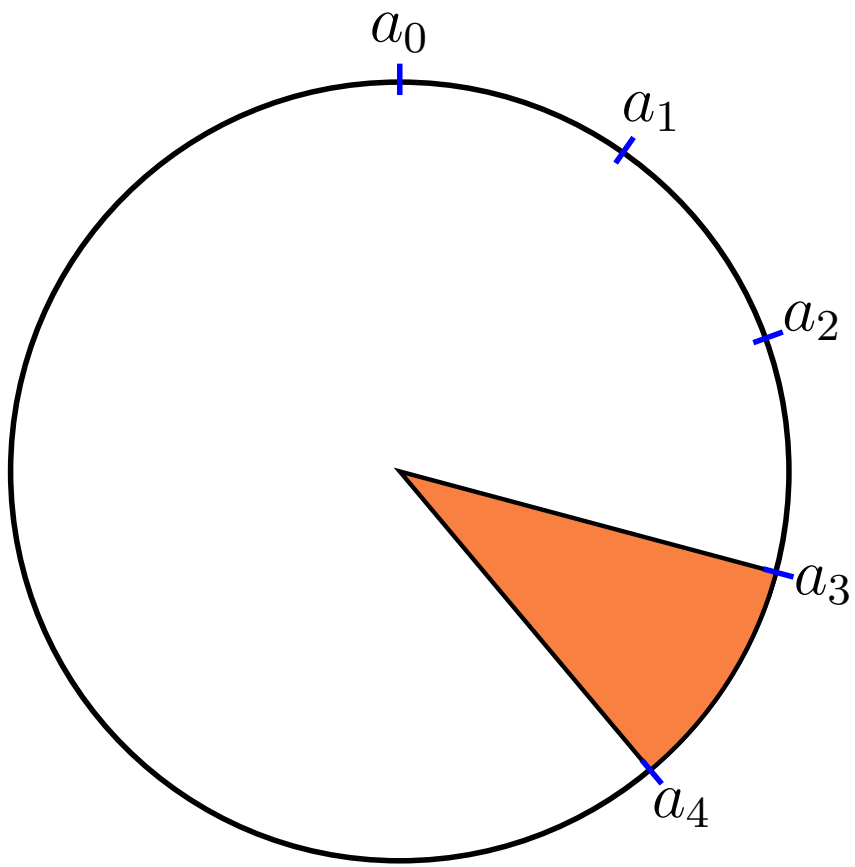
Théorèmes des 3 distances



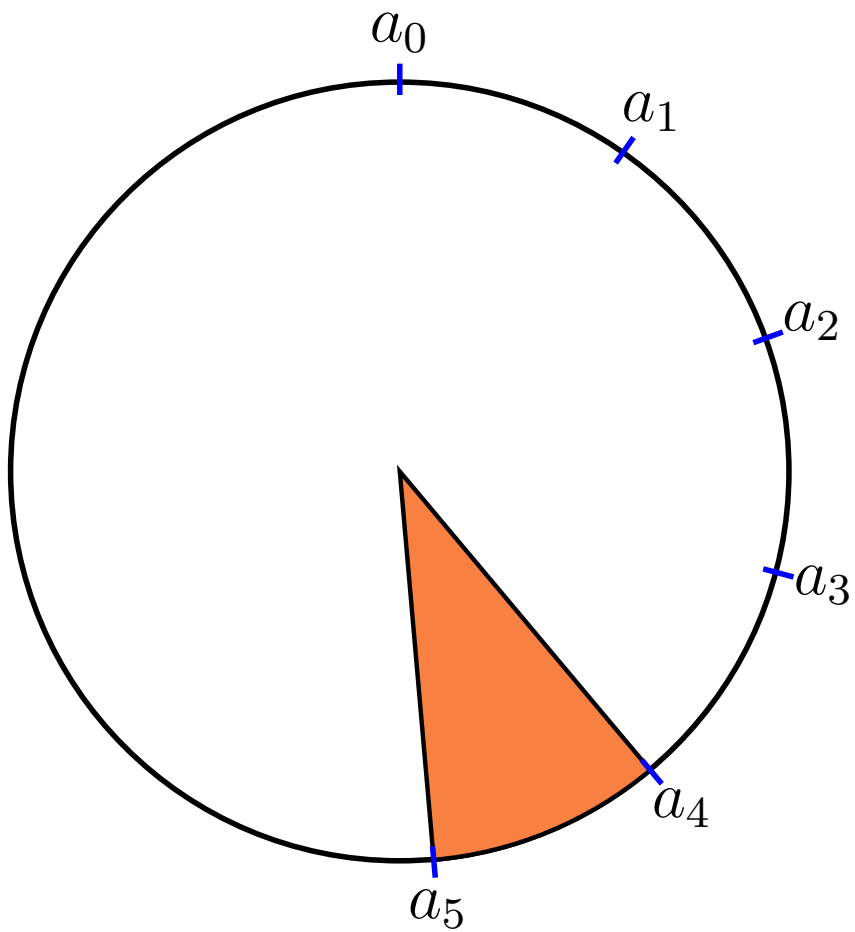
Théorèmes des 3 distances



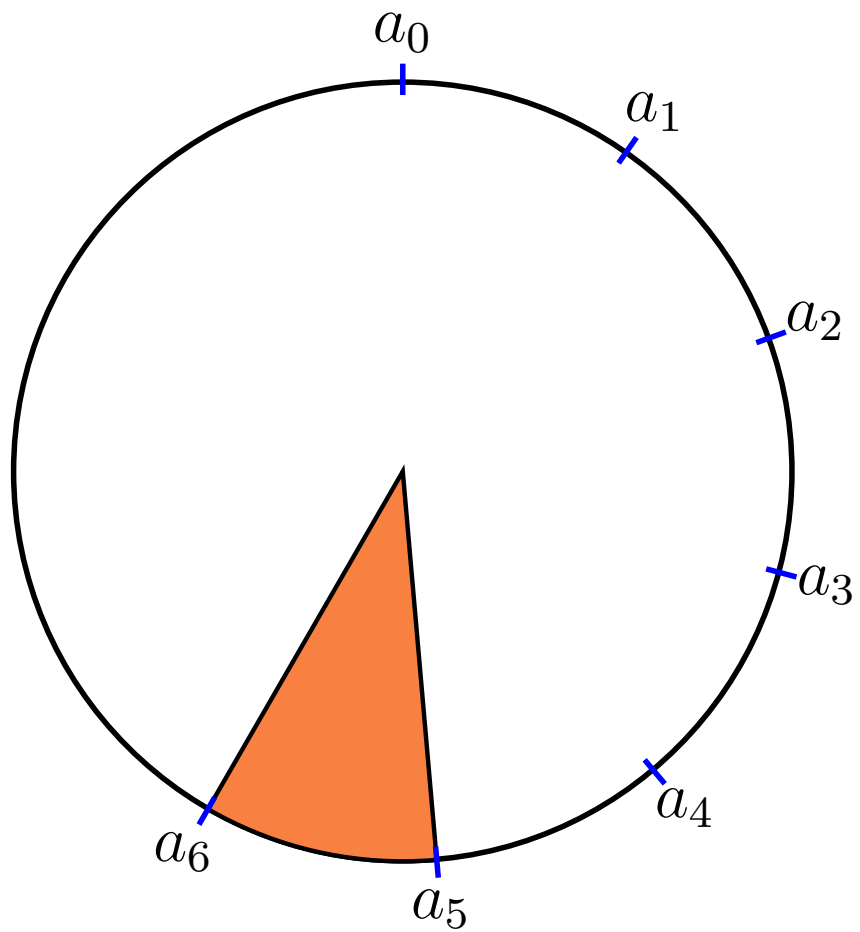
Théorèmes des 3 distances



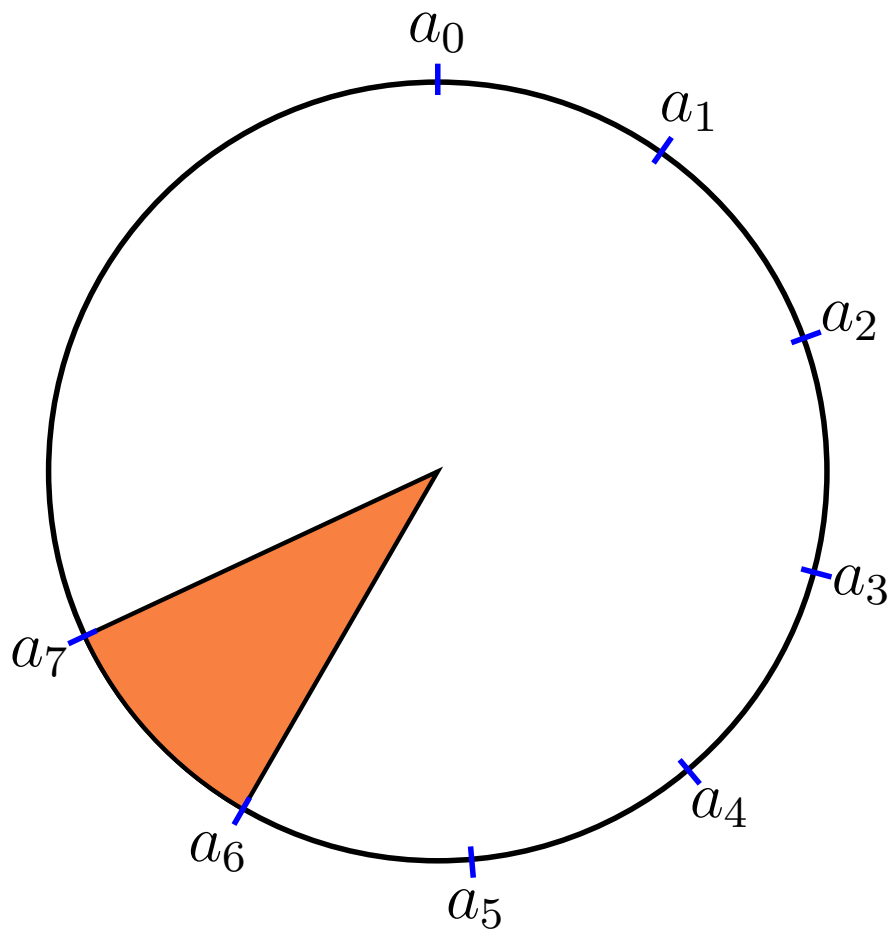
Théorèmes des 3 distances



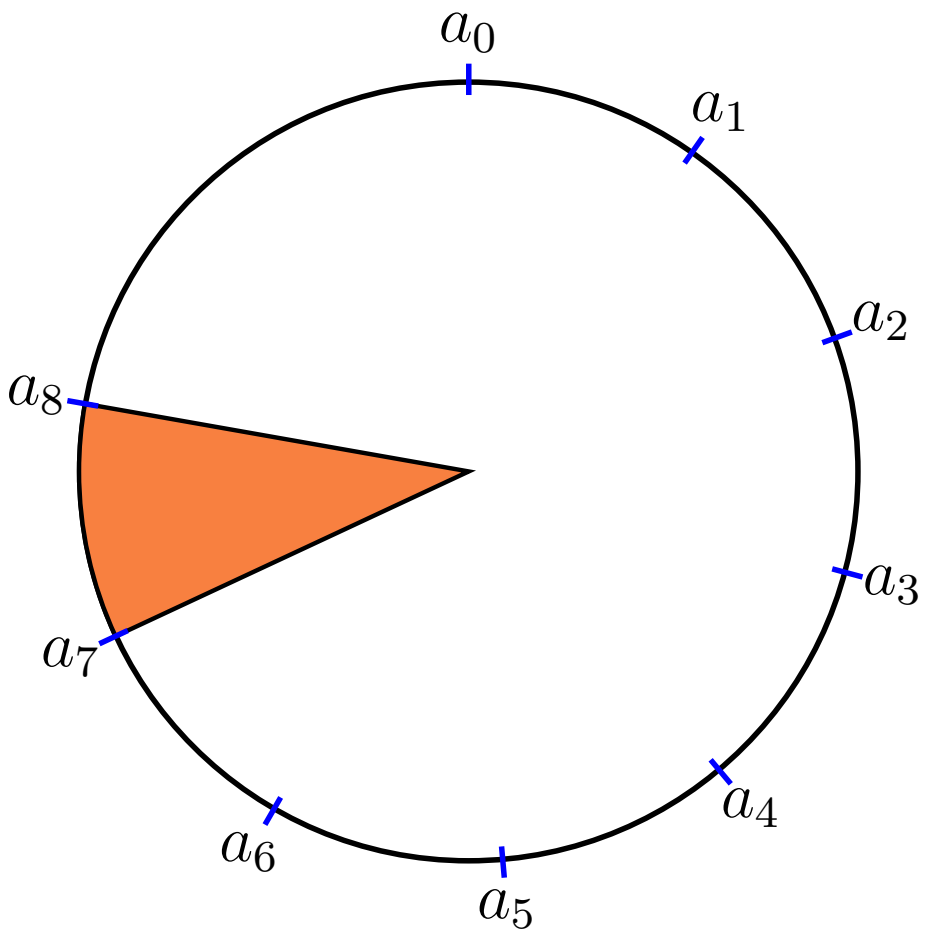
Théorèmes des 3 distances



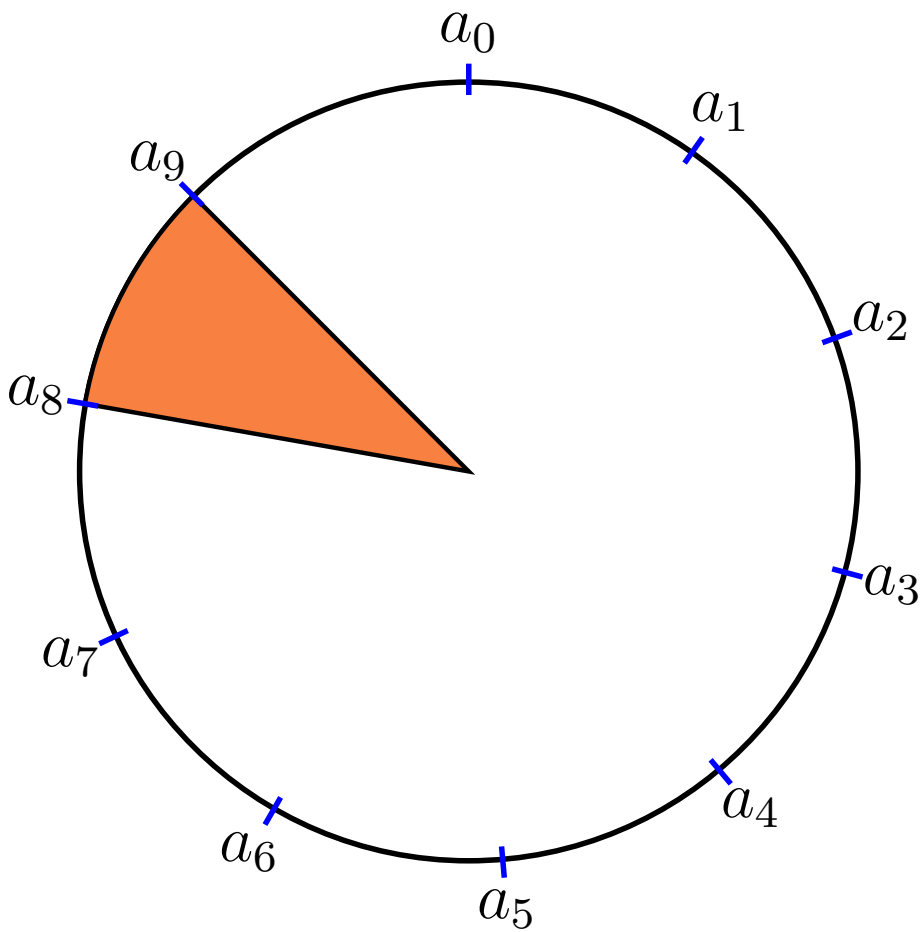
Théorèmes des 3 distances



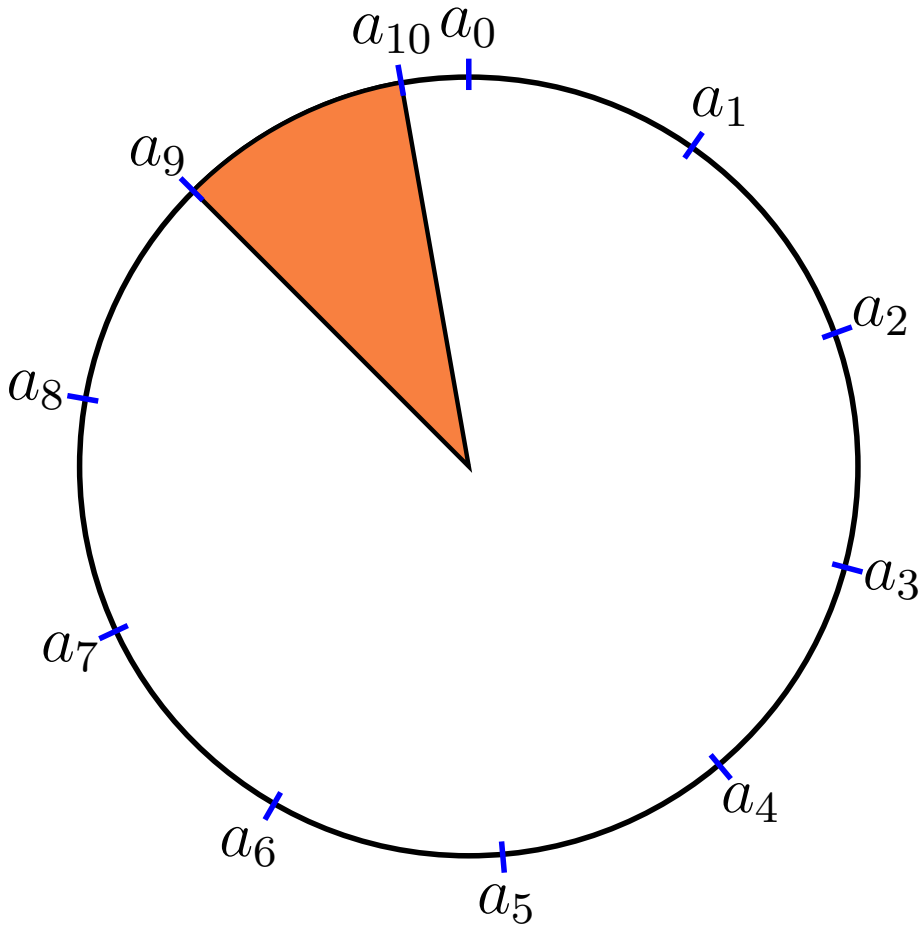
Théorèmes des 3 distances



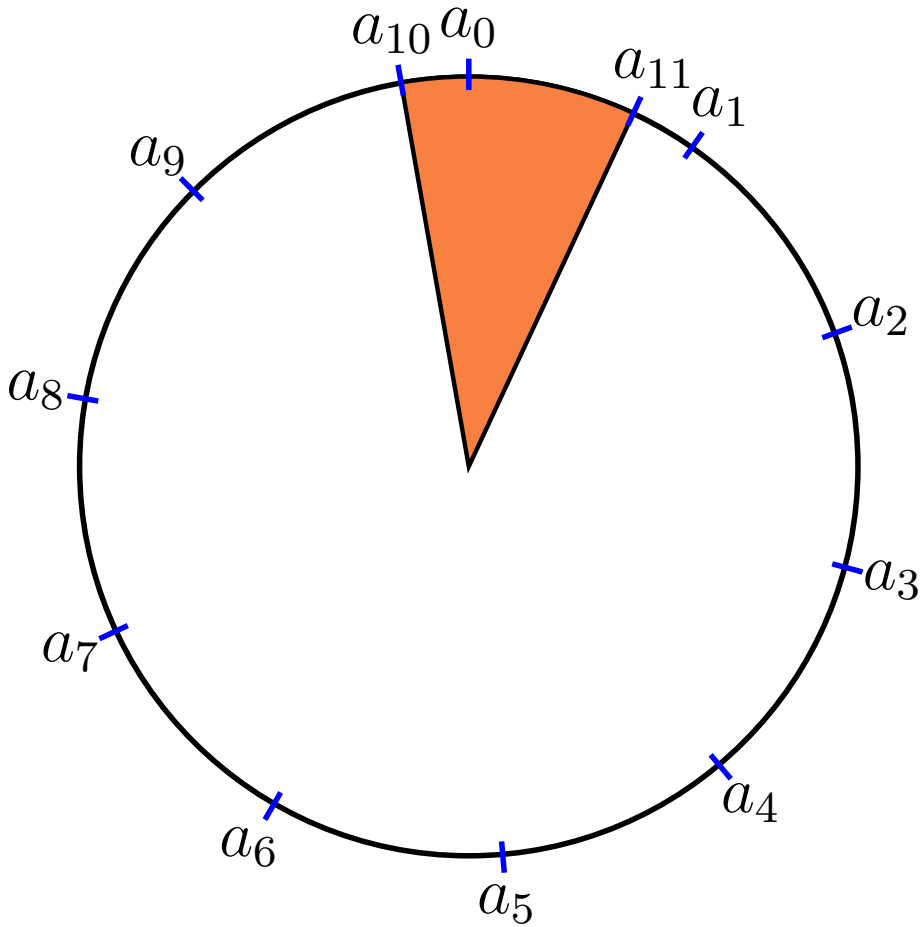
Théorèmes des 3 distances



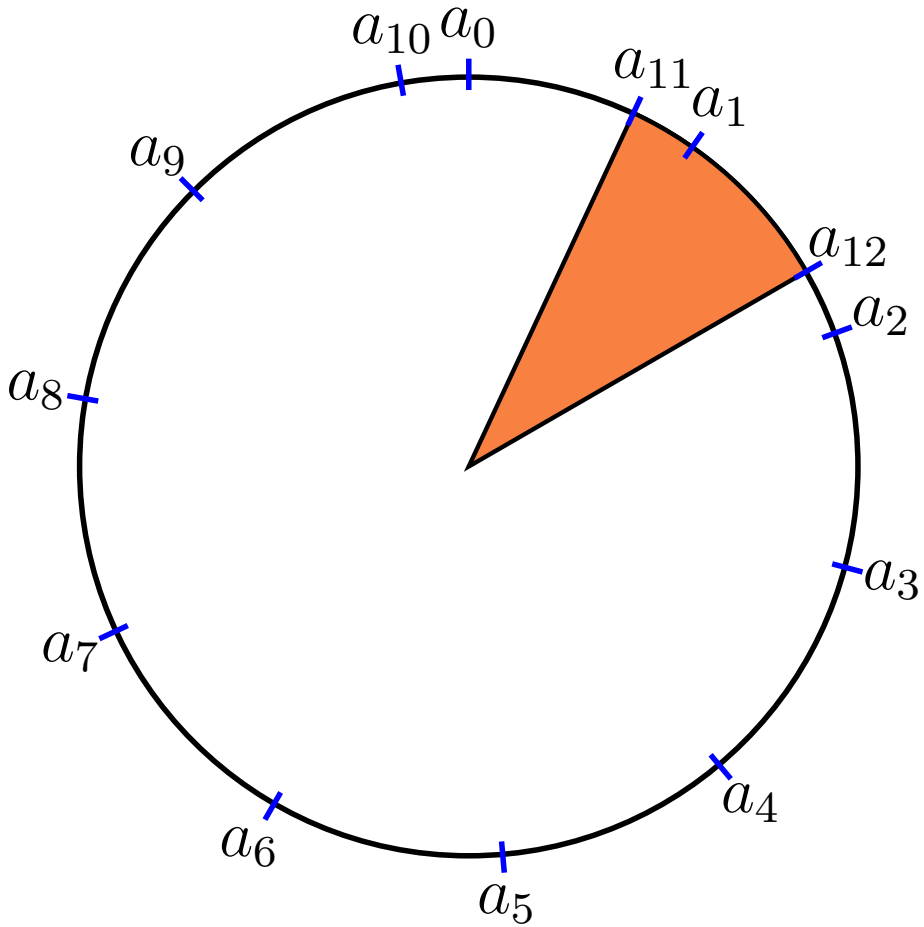
Théorèmes des 3 distances



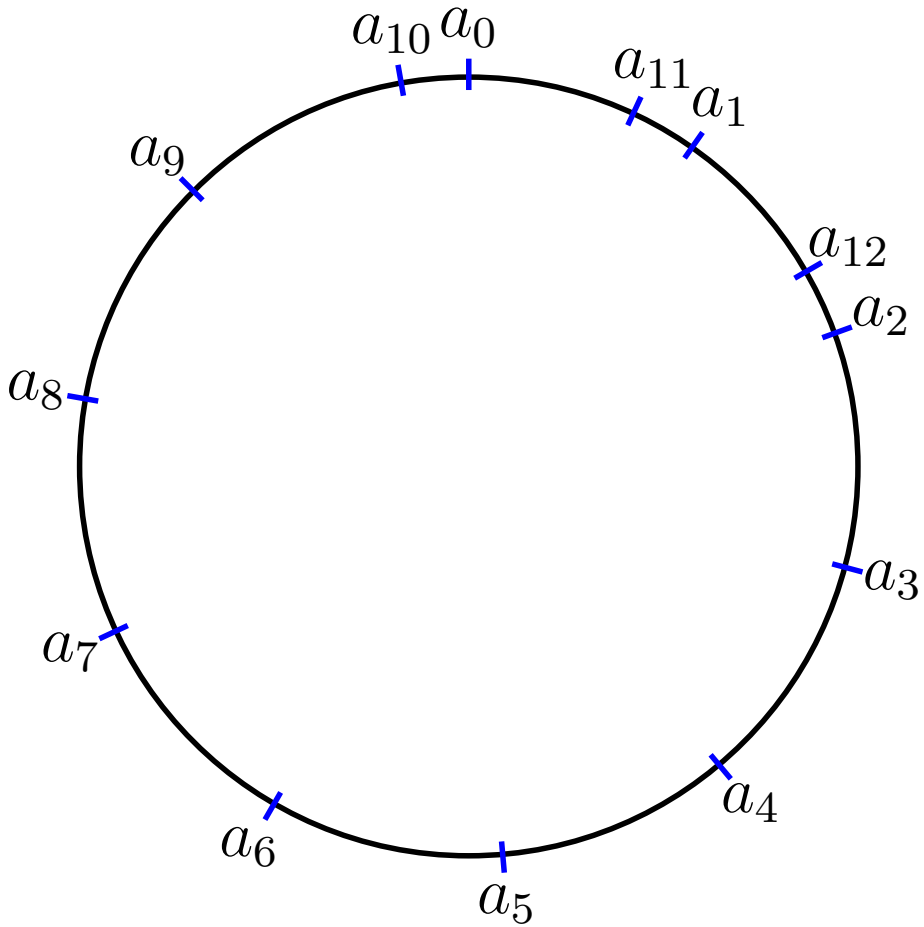
Théorèmes des 3 distances



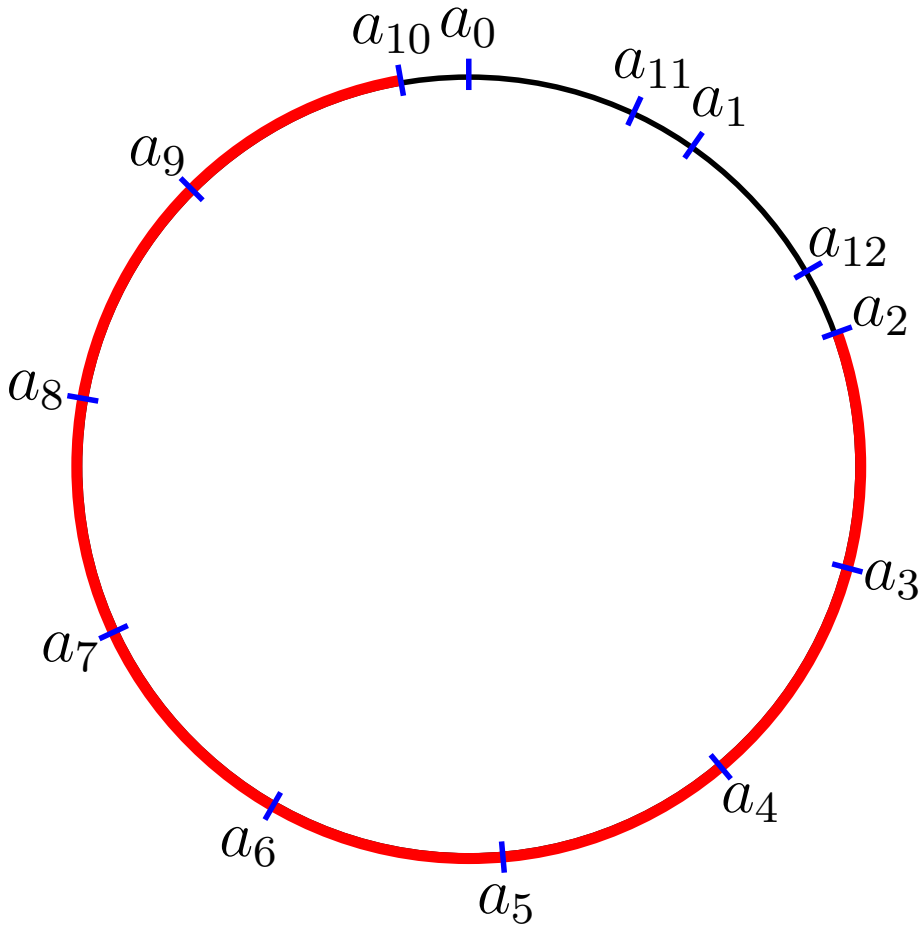
Théorèmes des 3 distances



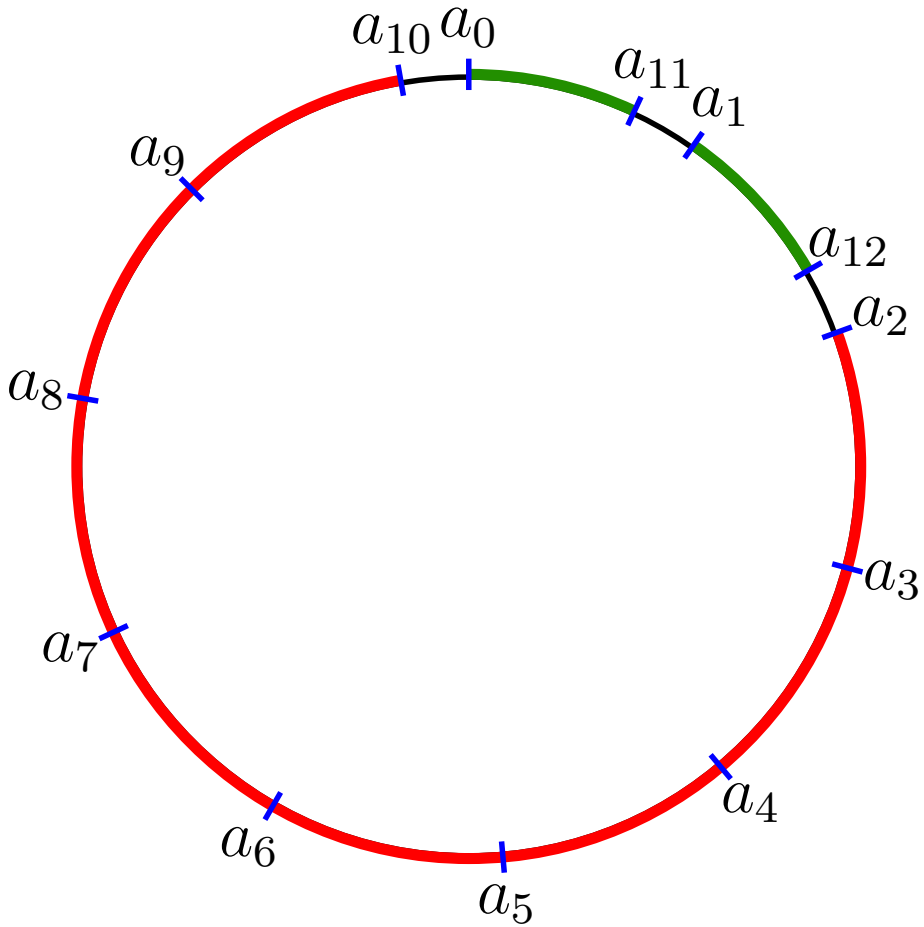
Théorèmes des 3 distances



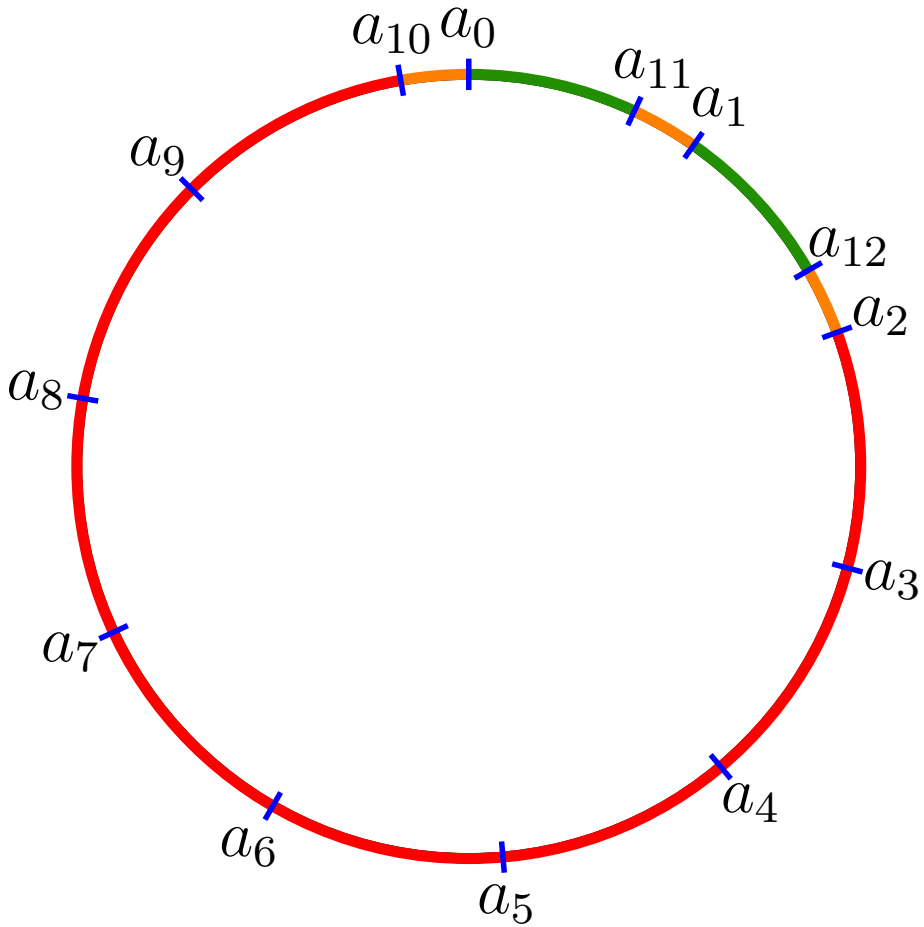
Théorèmes des 3 distances



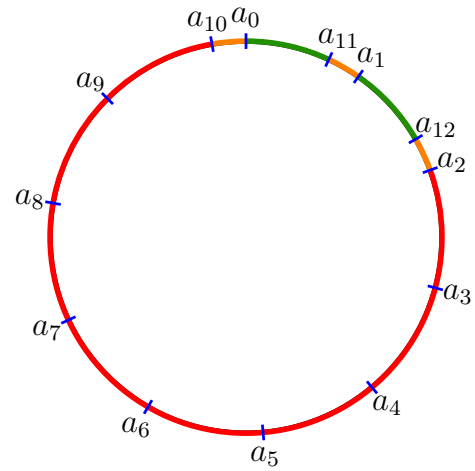
Théorèmes des 3 distances



Théorèmes des 3 distances

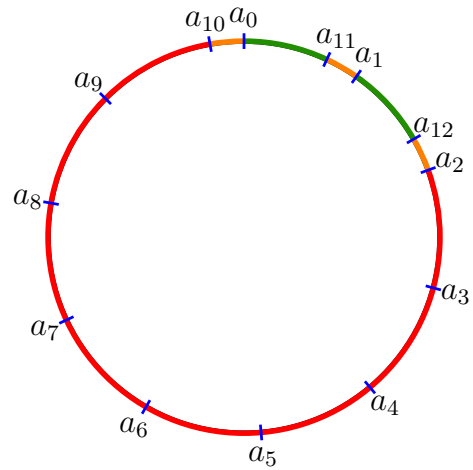


Théorèmes des 3 distances



Théorèmes des 3 distances

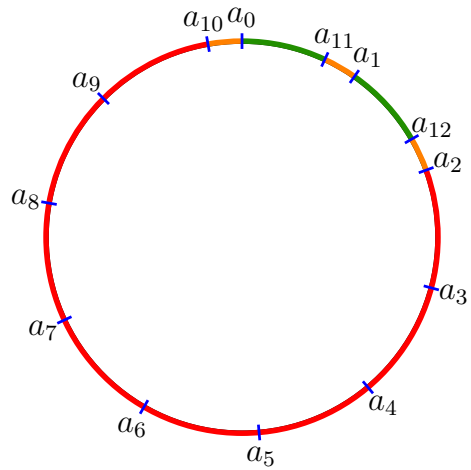
$\alpha \in \mathbb{R}$, $N \in \mathbb{N}, a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$



Théorèmes des 3 distances

$\alpha \in \mathbb{R}$, $N \in \mathbb{N}, a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$

next : $\overline{n}$, **pred** : $\underline{n}$, **min** : $m = \overline{0}$, **max** : $M = \underline{0}$

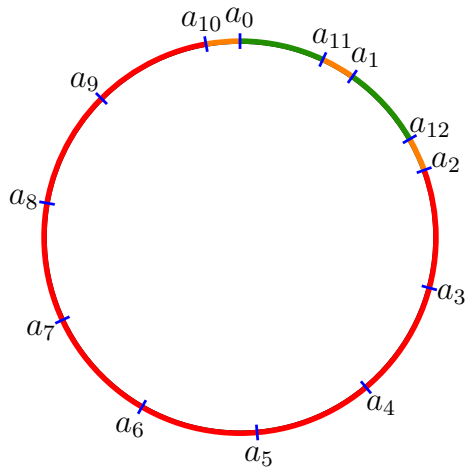


Théorèmes des 3 distances

$\alpha \in \mathbb{R}$, $N \in \mathbb{N}, a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$

next : $\overline{n}$, **pred** : $\underline{n}$, **min** : $m = \overline{0}$, **max** : $M = \underline{0}$

$\overline{12} = 2, \underline{12} = 1, m = 11, M = 10$



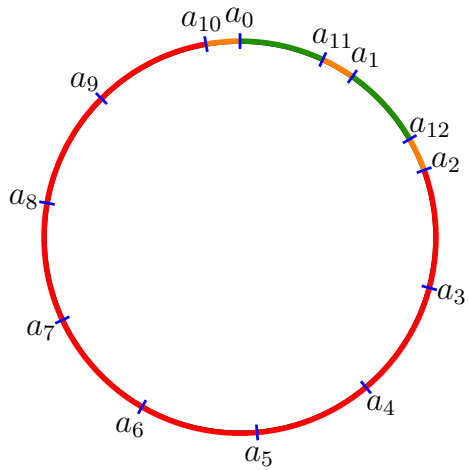
Théorèmes des 3 distances

$\alpha \in \mathbb{R}$, $N \in \mathbb{N}$, $a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$

next : $\overline{n}$, **pred** : $\underline{n}$, **min** : $m = \overline{0}$, **max** : $M = \underline{0}$

$\overline{12} = 2$, $\underline{12} = 1$, $m = 11$, $M = 10$

Si $n \leq N - m, \overline{n} = n + m,$ $\quad d = a_m$



Théorèmes des 3 distances

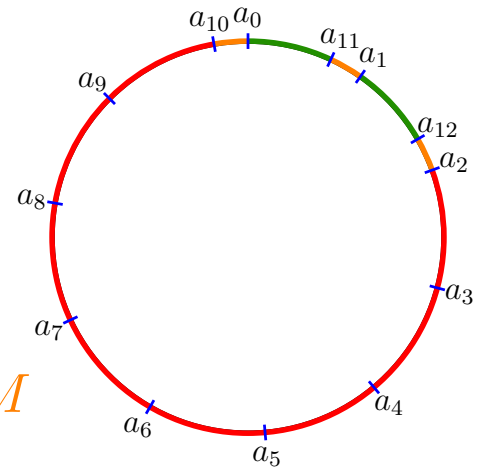
$\alpha \in \mathbb{R}$, $N \in \mathbb{N}, a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$

next : $\overline{n}$, **pred** : $\underline{n}$, **min** : $m = \overline{0}$, **max** : $M = \underline{0}$

$\overline{12} = 2, \underline{12} = 1, m = 11, M = 10$

Si $n \leq N - m, \overline{n} = n + m, \quad d = a_m$

Si $M < n \leq N, \overline{n} = n - M \quad d = 1 - a_M$



Théorèmes des 3 distances

$\alpha \in \mathbb{R}$, $N \in \mathbb{N}$, $a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$

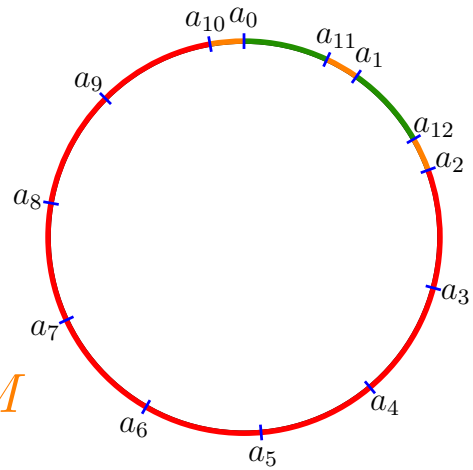
next : $\overline{n}$, **pred** : $\underline{n}$, **min** : $m = \overline{0}$, **max** : $M = \underline{0}$

$\overline{12} = 2$, $\underline{12} = 1$, $m = 11$, $M = 10$

Si $n \leq N - m, \overline{n} = n + m,$ $\quad d = a_m$

Si $M < n \leq N, \overline{n} = n - M$ $\quad d = 1 - a_M$

Si $N - a < n \leq M, \overline{n} = n + m - M$ $\quad d = 1 + a_m - a_M$

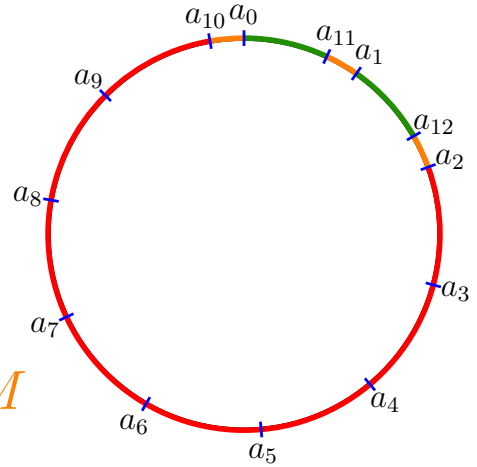


Théorèmes des 3 distances

$\alpha \in \mathbb{R}$, $N \in \mathbb{N}$, $a_n = \{\alpha n\}$, $a_n \neq 0$ **pour** $1 \leq n \leq N$

next : $\overline{n}$, **pred** : $\underline{n}$, **min** : $m = \overline{0}$, **max** : $M = \underline{0}$

$\overline{12} = 2$, $\underline{12} = 1$, $m = 11$, $M = 10$



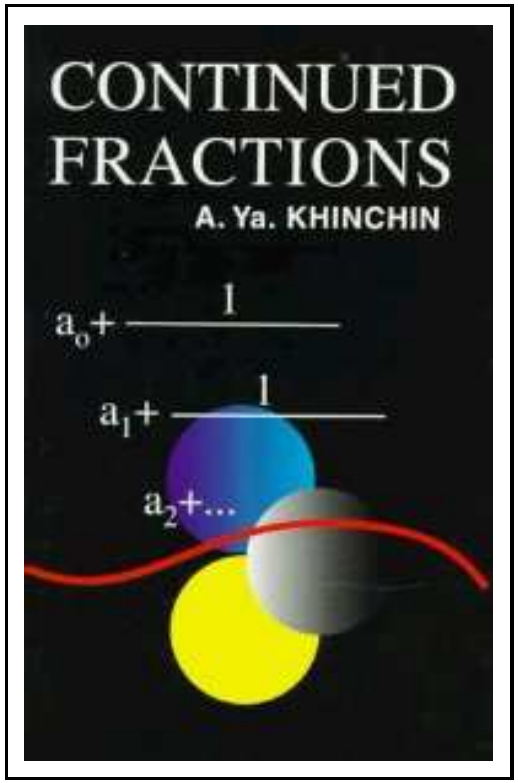
Si $n \leq N - m, \overline{n} = n + m, \quad d = a_m$

Si $M < n \leq N, \overline{n} = n - M \quad d = 1 - a_M$

Si $N - a < n \leq M, \overline{n} = n + m - M \quad d = 1 + a_m - a_M$

$[m\alpha]/m < \alpha < (1 + [M\alpha])/M$, $m(1 + [M\alpha]) - [m\alpha]M = 1$

Fraction continue



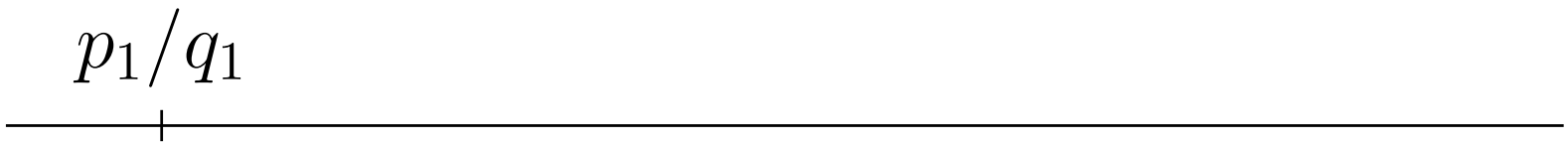
Fraction continue

Fraction continue

Médian

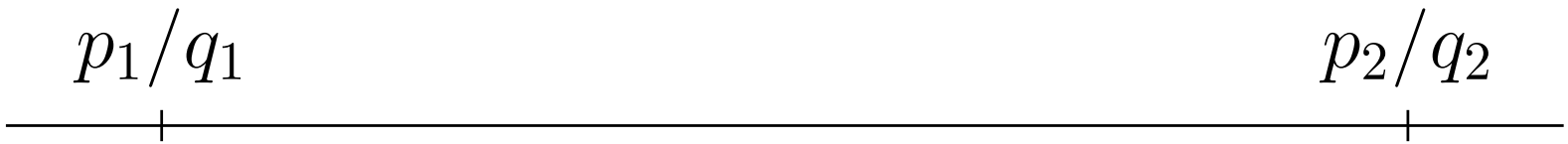
Fraction continue

Médian



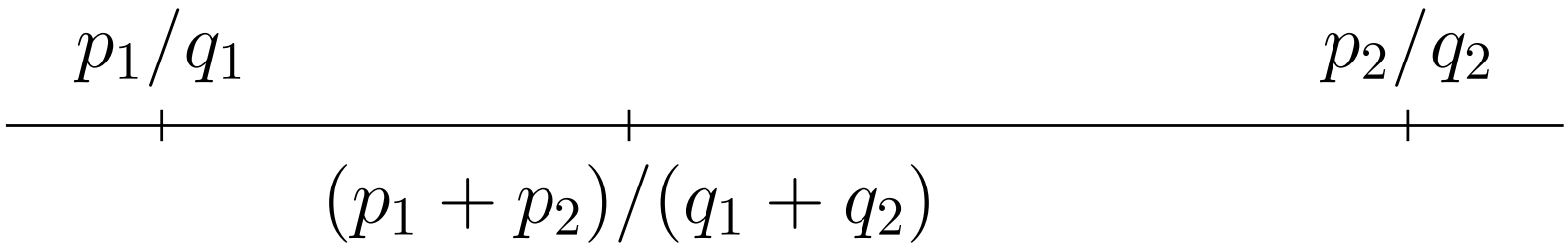
Fraction continue

Médian



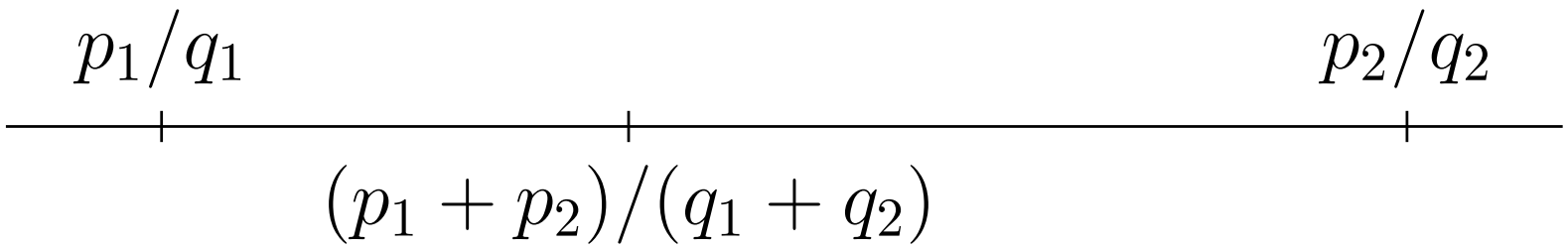
Fraction continue

Médian

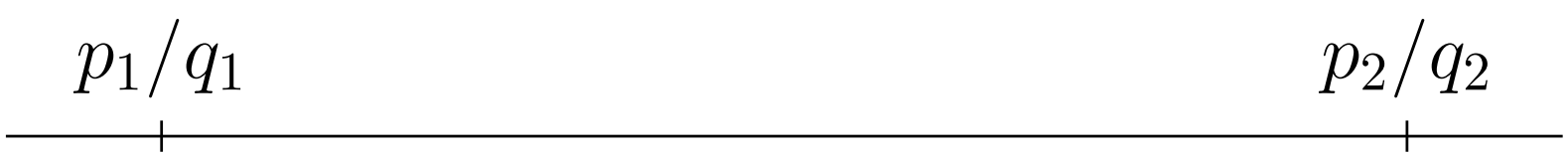


Fraction continue

Médian

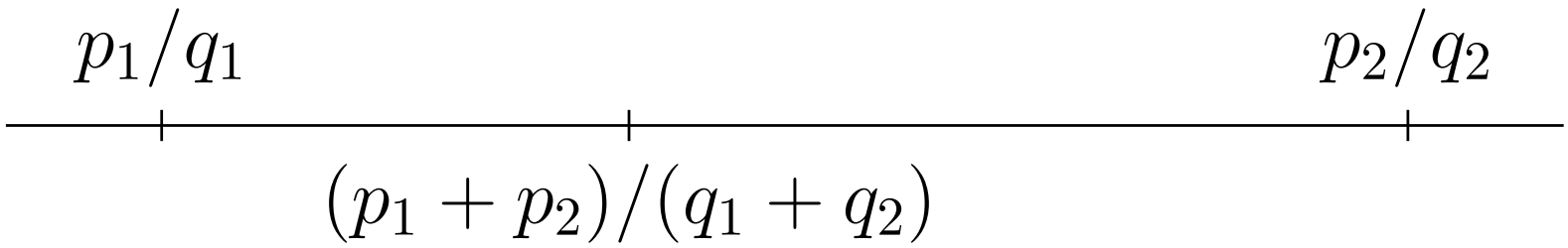


Approximation

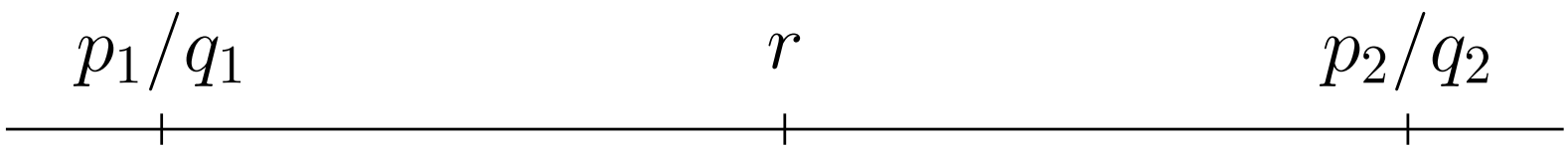


Fraction continue

Médian

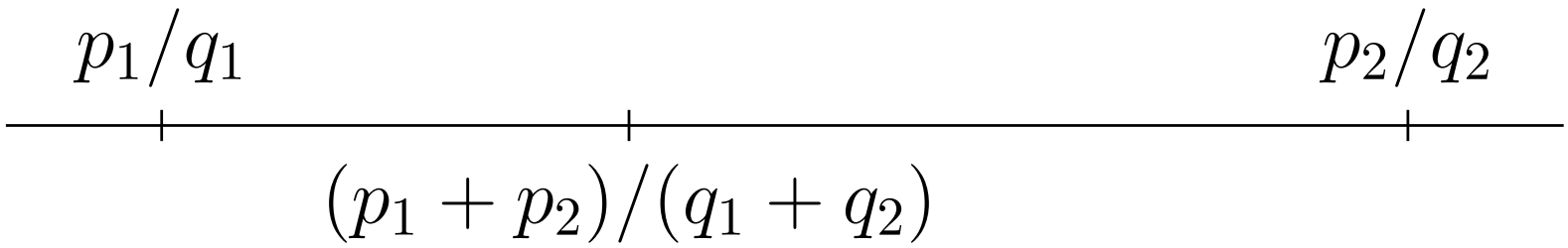


Approximation

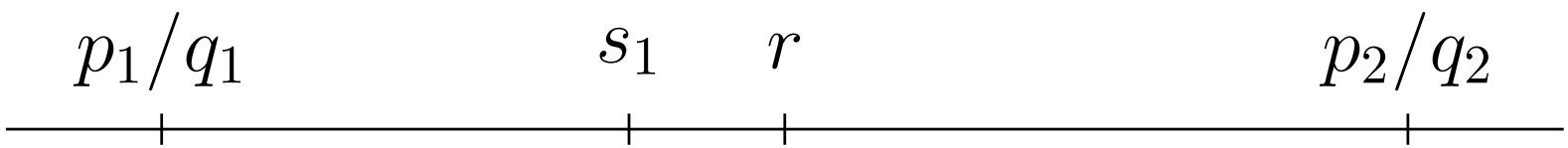


Fraction continue

Médian

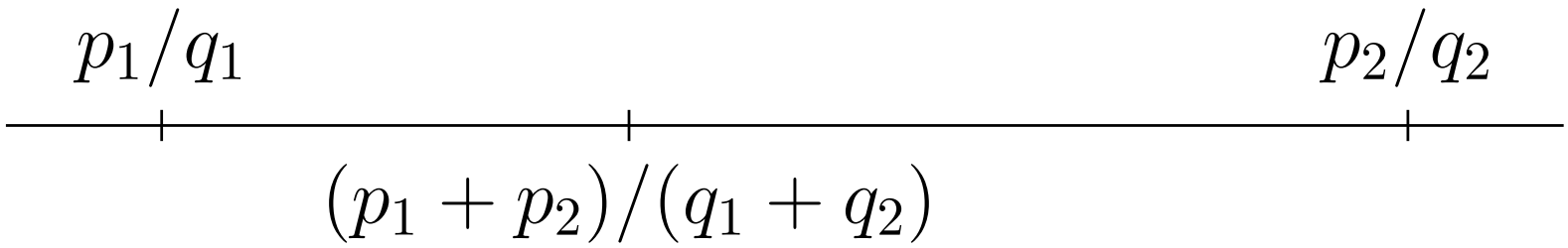


Approximation

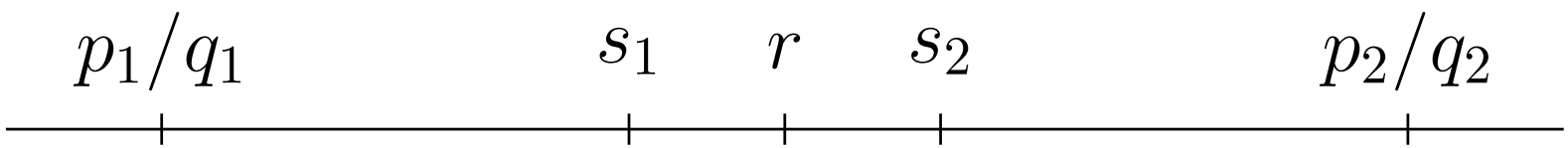


Fraction continue

Médian

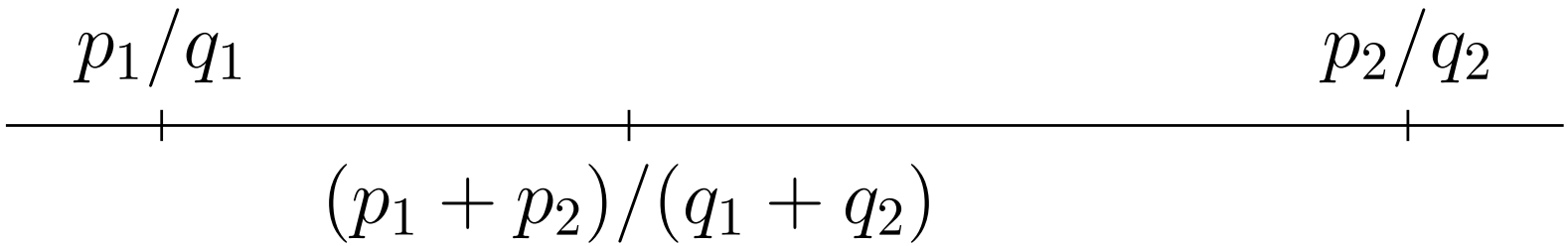


Approximation

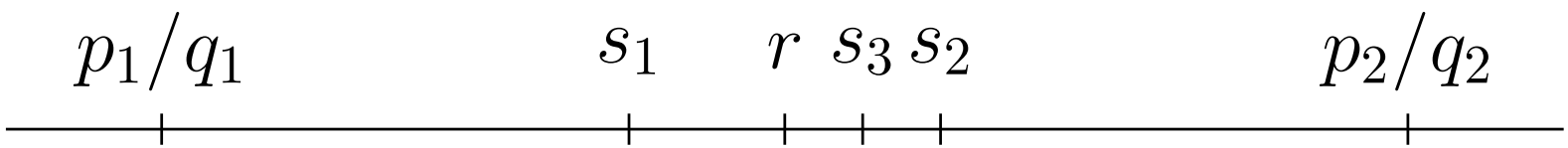


Fraction continue

Médian



Approximation



Fraction continue

Fraction continue

Fraction continue

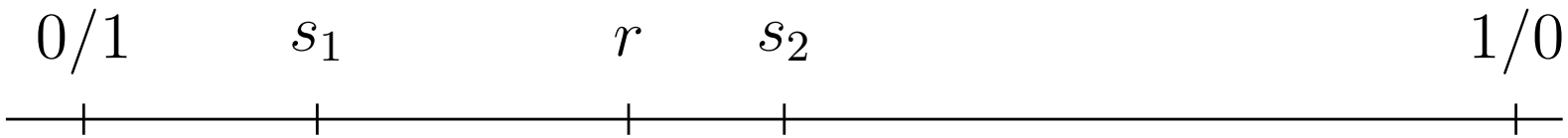
Fraction continue

Fraction continue

Fraction continue

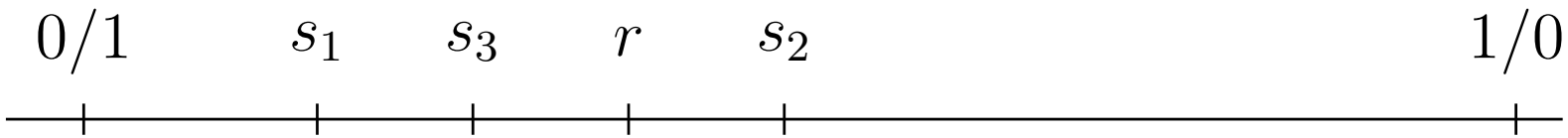
$s_1 = a_0$

Fraction continue



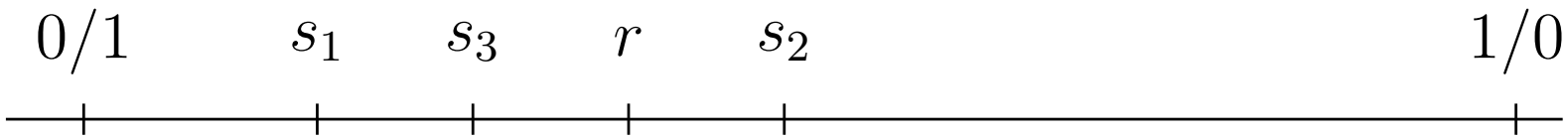
$s_1 = a_0$, $s_2 = a_0 + 1/a_1$

Fraction continue



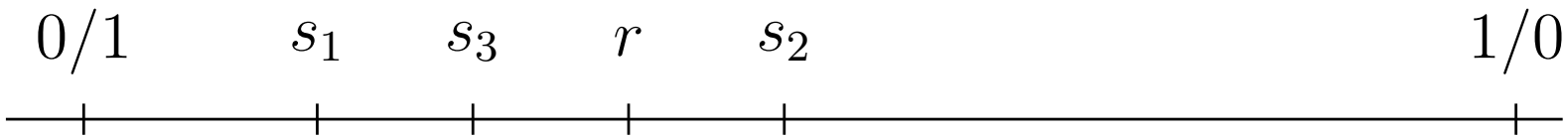
$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$

Fraction continue



$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$, ...

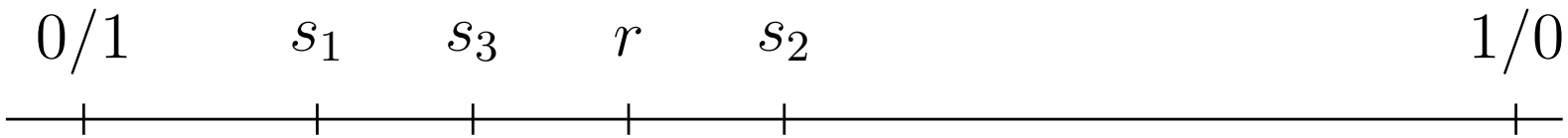
Fraction continue



$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$, ...

$r \rightsquigarrow [a_0; a_1; a_2; \ldots]$

Fraction continue

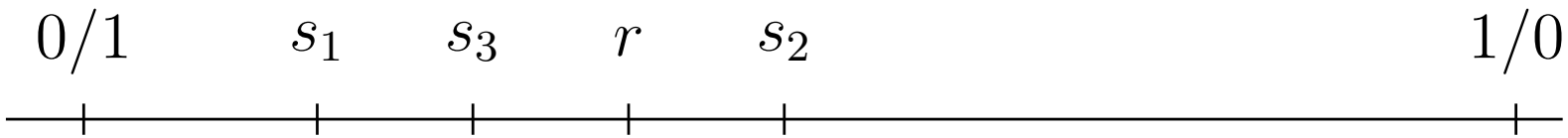


$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$, ...

$r \rightsquigarrow [a_0; a_1; a_2; \ldots]$

convergent $s_n = p_n/q_n$

Fraction continue



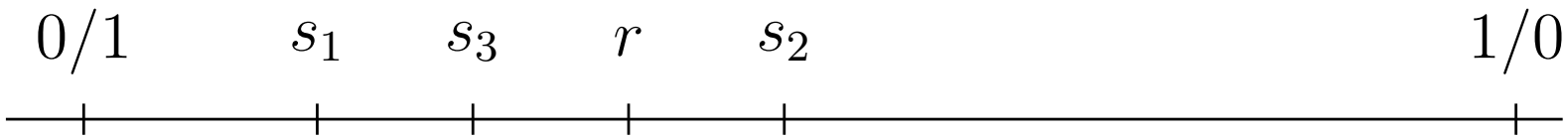
$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$, ...

$r \rightsquigarrow [a_0; a_1; a_2; \ldots]$

convergent $s_n = p_n/q_n$

numérateur $p_0 = 1$, $p_1 = a_0$, $p_{n+2} = a_{n+1}p_{n+1} + p_n$

Fraction continue



$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$, ...

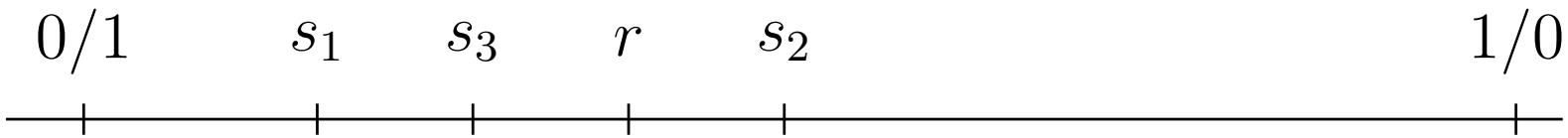
$r \rightsquigarrow [a_0; a_1; a_2; \ldots]$

convergent $s_n = p_n/q_n$

numérateur $p_0 = 1$, $p_1 = a_0$, $p_{n+2} = a_{n+1}p_{n+1} + p_n$

dénominateur $q_0 = 0$, $q_1 = 1$, $q_{n+2} = a_{n+1}q_{n+1} + q_n$

Fraction continue



$s_1 = a_0$, $s_2 = a_0 + 1/a_1$, $s_3 = a_0 + 1/(a_1 + 1/a_2)$, ...

$r \rightsquigarrow [a_0; a_1; a_2; \ldots]$

convergent $s_n = p_n/q_n$

numérateur $p_0 = 1$, $p_1 = a_0$, $p_{n+2} = a_{n+1}p_{n+1} + p_n$

dénominateur $q_0 = 0$, $q_1 = 1$, $q_{n+2} = a_{n+1}q_{n+1} + q_n$

convergent interm. $s_{n,i} = (ip_{n+1} + p_n)/(iq_{n+1} + q_n)$, $0 \leq i \leq a_{n+1}$

Fraction continue

Meilleure approximation : a/b pour r

Fraction continue

Meilleure approximation : a/b **pour** r

$c/d \neq a/b$ **et** $0 < d \leq b$ **,** $|r - a/b| < |r - c/d|$

Fraction continue

Meilleure approximation : a/b pour r

$c/d \neq a/b$ et $0 < d \leq b$, $|r - a/b| < |r - c/d|$

$\rightsquigarrow a/b$ est un convergent intermédiaire.

Fraction continue

Meilleure approximation : a/b **pour** r

$c/d \neq a/b$ **et** $0 < d \leq b$ **,** $|r - a/b| < |r - c/d|$

$\rightsquigarrow a/b$ **est un convergent intermédiaire.**

$c/d \neq a/b$ **et** $0 < d \leq b$ **,** $|br - a| < |dr - c|$

Fraction continue

Meilleure approximation : a/b pour r

$c/d \neq a/b$ et $0 < d \leq b$, $|r - a/b| < |r - c/d|$

$\rightsquigarrow a/b$ est un convergent intermédiaire.

$c/d \neq a/b$ et $0 < d \leq b$, $|br - a| < |dr - c|$

$\leftrightsquigarrow a/b$ est un convergent.

Ce qui reste à faire

Réduction

Réduction

$f(x)$ est très proche d'un flottant pour $x \in I$

Réduction

$f(x)$ est très proche d'un flottant pour $x \in I$

Approximer f par un $P \rightsquigarrow \epsilon_1$

Réduction

$f(x)$ est très proche d'un flottant pour $x \in I$

Approximer f par un $P \rightsquigarrow \epsilon_1$

Prendre les deux premiers termes de $P \rightsquigarrow \epsilon_2$

Réduction

$f(x)$ est très proche d'un flottant pour $x \in I$

Approximer f par un $P \rightsquigarrow \epsilon_1$

Prendre les deux premiers termes de $P \rightsquigarrow \epsilon_2$

Faire un changement de variable : $b - ax$, $x \leq N$

Réduction

$f(x)$ est très proche d'un flottant pour $x \in I$

Approximer f par un $P \rightsquigarrow \epsilon_1$

Prendre les deux premiers termes de $P \rightsquigarrow \epsilon_2$

Faire un changement de variable : $b - ax$, $x \leq N$

$\texttt{inf}\{b - ax \mod 1| \leq N\} < \epsilon$?

Numération d'Ostrowski

Numération d'Ostrowski

$$\theta_n = (-1)^n(\alpha q_n - p_n), \theta_n < 1/q_{n+1}$$

Numération d'Ostrowski

$$\theta_n = (-1)^n(\alpha q_n - p_n), \theta_n < 1/q_{n+1}$$

$$q_n\theta_n + q_{n+1}\theta_{n+1} = 1$$

Numération d'Ostrowski

$$\theta_n = (-1)^n(\alpha q_n - p_n), \theta_n < 1/q_{n+1}$$

$$q_n\theta_n + q_{n+1}\theta_{n+1} = 1$$

$$b = \sum_i b_i\theta_i$$

Numération d'Ostrowski

$\theta_n = (-1)^n(\alpha q_n - p_n)$, $\theta_n < 1/q_{n+1}$

$q_n\theta_n + q_{n+1}\theta_{n+1} = 1$

$b = \sum_i b_i\theta_i$

Comment calculer $r_n = \beta - \sum_{i<n} b_i\theta_i$?

Numération d'Ostrowski

$\theta_n = (-1)^n(\alpha q_n - p_n)$, $\theta_n < 1/q_{n+1}$

$q_n\theta_n + q_{n+1}\theta_{n+1} = 1$

$b = \sum_i b_i\theta_i$

Comment calculer $r_n = \beta - \sum_{i<n} b_i\theta_i$?