The Three Gap theorem (Steinhaus conjecture)

Micaela Mayero*

INRIA-Rocquencourt**

Abstract. We deal with the distribution of N points placed consecutively around the circle by a fixed angle of α. From the proof of Tony van Ravenstein [RAV88], we propose a detailed proof of the Steinhaus conjecture whose result is the following: the N points partition the circle into gaps of at most three different lengths.
We study the mathematical notions required for the proof of this theorem revealed during a formal proof carried out in Coq.

Introduction

Originally, the three gap theorem was the conjecture of H. Steinhaus. Subsequently, several proofs were proposed by [SOS57] [SOS58] [SWI58] [SUR58] [HAL65] [SLA67] [RAV88]. The proof proposed in this paper is a presentation of the proof completely fomalized in the Coq proof asssistance system [MAY99]. This formal proof is based on Tony van Ravenstein's [RAV88].

This kind of demostration, which involves geometrical intuition, is a real challenge for proof assistance systems. That is what motivated our work. Therefore, the interest of such an approach is to understand, by means of an example, if the Coq system allows us to prove a theorem coming from pure mathematics.
In addition, this development allowed us to clarify some points of the proof and has led to a more detailed proof.

First, we will define the notations and definitions used for stating and proving this theorem.The second part deals with different states of the theorem and with the proof itself. Finally, the last part presents advantages of the formal proof stating the main differences between our proof and Tony van Ravenstein's proof.

1 Notations and definitions

1.1 Notations

We can refer to figure 1.

* Micaela.Mayero@inria.fr, http://coq.inria.fr/~mayero/

** Projet Coq, INRIA-Rocquencourt, domaine de Voluceau, B.P. 105, 78153 Le Chesnay Cedex, France.

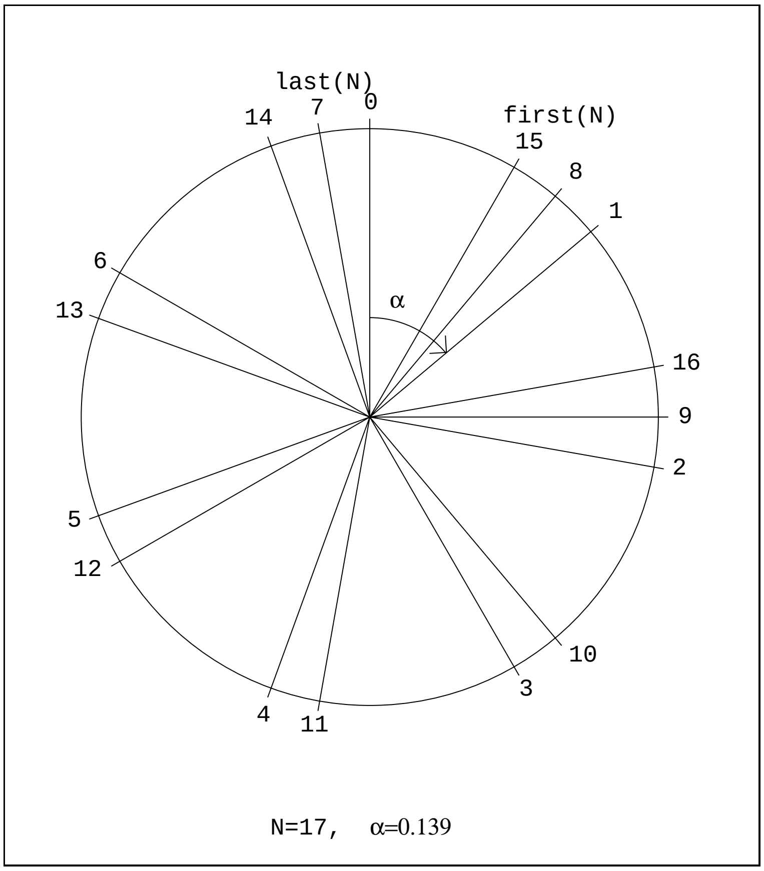

Fig. 1. The three gap theorem

- $\mathbb{N}$ is the natural numbers set.
- $\mathbb{R}$ is the real numbers set.
- The integer part of a real number r is noted $E(r)$.
- The fractional part of a real number r, ie $r - E(r)$, is written $\{r\}$.
- The first point on the circle is the point 0.
- Unless explicitly mentioned, we consider N points distributed around the circle. These are numbered from 0 to $N - 1$.
- We consider the circle of **unit circumference** and with a clockwise orientation.
- α is counted in turns of the circle (and not in radian); then $0 \leq \alpha < 1$.
- The first point ($\neq 0$ if $N >$1) on the right of 0 is written $first(N)$. $first(N)$ is a function from the natural numbers to the natural numbers.
- The last point ($\neq 0$ if $N >$1) before 0 is written $last(N)$. $last(N)$ is a function from the natural numbers to the natural numbers.
- $n \in Circle$ is equivalent to $0 \leq n < N$.

Remark 1. The distance from point 0 to point n is $\{n.\alpha\}$.

1.2 Definitions

The following definitions are valid for all α, rational or irrational.

Lemma 1 (Existence of first). *If $N \geq 2$ then there exists an integer $first(N) \in \mathbb{N}$ s.t. $0 < first(N) < N$ and $\forall m \in \mathbb{N}$ if $0 < m < N$ then $\{first(N).\alpha\} \leq \{m.\alpha\}$*

Proof.
By induction on N.
- $N = 2$: in this case $first(N) = 1$.
- Suppose the lemma to be holds for N: then there exists $first(N) \in \mathbb{N}$ s.t. $0 < first(N) < N$ and $\forall m \in \mathbb{N}$ if $0 < m < N$ then $\{first(N).\alpha\} \leq \{m.\alpha\}$;
let us show that there exists $first(N+1) \in \mathbb{N}$ s.t. $0 < first(N+1) < N+1$ and $\forall m \in \mathbb{N}$ if $0 < m < N+1$ then $\{first(N+1).\alpha\} \leq \{m.\alpha\}$.
By cases:
   - if $\{first(N).\alpha\} \leq \{N.\alpha\}$ then $first(N+1) = first(N)$.
   - if $\{first(N).\alpha\} > \{N.\alpha\}$ then $first(N) = N$.

□

Lemma 2 (Existence of last). *If $N \geq 2$ then there exists an integer $last(N) \in \mathbb{N}$ s.t. $0 < last(N) < N$ and $\forall m \in \mathbb{N}$ if $0 < m < N$ then $\{m.\alpha\} \leq \{last(N).\alpha\}$*

Proof.
Symmetrical proof with respect to first.

□

The successor of a point on the circle ($after$) verifies the following property:

Lemma 3 (Property of points for after). *$\forall M \in \mathbb{R}$ if $0 \leq M < 1$ then we have:*
   either
1. *there exists an integer $I \in \mathbb{N}$ s.t. $0 < I < N$ and $M < \{I.\alpha\}$ and $\forall m \in \mathbb{N}$ if $0 \leq m < N$ and if $\{m.\alpha\} > M$ then $\{m.\alpha\} \geq \{I.\alpha\}$*
   or
2. *$\forall m \in \mathbb{N}$ if $0 \leq m < N$ then $0 \leq \{m.\alpha\} \leq M$*

Proof.
By induction on N.
- $N = 1$: 0 verifies the property.
- Suppose lemma to holds for N and prove it for $N+1$: the induction hypothesis is the following:
either
1. there exists an integer $I(N) \in \mathbb{N}$ s.t. $0 < I(N) < N$ and $M < \{I(N).\alpha\}$ and

$\forall m \in \mathbb{N}$ if $0 \leq m < N$ and if $\{m.\alpha\} > M$ then $\{m.\alpha\} \geq \{I(N).\alpha\}$
or
2. $\forall m \in \mathbb{N}$ if $0 \leq m < N$ then $0 \leq \{m.\alpha\} \leq M$
We prove that :
either

1. there exists an integer $I(N+1) \in \mathbb{N}$ s.t. $0 < I(N+1) < N+1$ and $M < \{I(N+1).\alpha\}$ and $\forall m \in \mathbb{N}$ if $0 \leq m < N+1$ and if $\{m.\alpha\} > M$ then $\{m.\alpha\} \geq \{I(N+1).\alpha\}$

or

2. $\forall m \in \mathbb{N}$ if $0 \leq m < N+1$ then $0 \leq \{m.\alpha\} \leq M$

By cases:

- if $0 \leq M < \{N.\alpha\}$ we are in case 1 and we continue by cases:
  - if $\{N.\alpha\} < \{I(N).\alpha\}$ then $I(N+1) = N$.
  - if $\{I(N).\alpha\} \leq \{N.\alpha\}$ then $I(N+1) = I(N)$.
- if $\{N.\alpha\} \leq M < 1$ we are in case 2 and the proof is immediate by induction hypothesis.

□

Definition 1 (after). *For all points n on the circle, the point $after(N, n)$ verifies the property of points (lemma 3) for $M = \{n.\alpha\}$ and is defined such that:*
if we are in case 1. then $after(N, n) = I$
if we are in case 2. then $after(N, n) = 0$.

2 Statement and proof of the theorem

2.1 Statement

Statement in natural language:

Theorem 1 (Intuitive statement). *Let N points be placed consecutively around the circle by an angle of α. Then for all irrational α and natural N, the points partition the circle into gaps of at most three different lengths.*

As shown by theorem 1 the points are numbered in order of apparition; now, if we do more than one revolution around the circle, new points appear between the former points. Then, when the last point $(N-1)$ is placed, it is possible to number them again consecutively and clockwise. In this new numeration, we use only the definitions of $first$, $last$ and $after$, from lemmas 1 and 2, and of the definition 1.

If we set $\|x\| = min(\{x\}, 1 - \{x\})$, then the distance of a point n from its successor $after(N, n)$ is given by $\|after(N, n) - n\|$. In order to show that this function can have at most three values, we show that the function $(after(N, n) - n)$ can itself have at most three values.

So, proving theorem 1 comes to the same thing as showing the following mathematical formulation, which we will prove in the next paragraph.

Theorem 2 (The three gap theorem).

$$after(N,m)-m=\begin{cases} first(N) & \textit{if } 0\le m<N-first(N)\\ first(N)-last(N) & \textit{if } N-first(N)\le m<last(N)\\ -last(N) & \textit{if } last(N)\le m<N\end{cases}$$

Remark 2.

1. This transcription means that the circle of N points is divided into
   $N-first$ gaps of length $\|first.\alpha\,\|$,
   $N-last$ gaps of length $\|last.\alpha\,\|$ and
   $first+last-N$ gaps of length $\|first.\alpha\,\|+\|last.\alpha\,\|$.
2. Theorem 2 is true for α rational and irrational. Here, however, we present only the proof for α irrational. Indeed, most of the intermediate results are false for α rational (among other reasons because $first$, $last$ and $after$ are no longer functions). Moreover, the theorem is trivially true for α rational: if $\alpha=p/q$ then the circle may include one or two lengths of gap - depending on whether $N<q$ or $N=q$.

2.2 Proof

We recall that the proof is detailed for α irrational and $N\ge 2$.

Lemma 4 (particular case). *If* $N=first(N)+last(N)$

$$after(N,m)-m=\begin{cases} first(N) & \textit{if } 0\le m<last(N)\\ -last(N) & \textit{if } last(N)\le m<N\end{cases}$$

Proof.

1. Case $0\le m<last(N)$:
   For $m=0$, by definition of first we have $after(N,0)=first(N)$.

   We want to prove that $m+first(N)$ is the successor of m.
   Let us first show that $m+first(N)$ belongs to the circle of N points: if $0<m<last(N)$ then
   $0<0+first(N)\le m+first(N)<last(N)+first(N)=N$.

   Now, let us show that: if i is any point of the circle $(0<i<N)$ then we have either $\{i.\alpha\}<\{m.\alpha\}$ or $\{i.\alpha\}>\{(m+first(N)).\alpha\}$.
   By reductio ad absurdum and by cases:
   let us suppose that $\{m.\alpha\}<\{i.\alpha\}<\{(m+first(N)).\alpha\}$

- if $i > m$ then $0 < \{i.\alpha\} - \{m.\alpha\} < \{(m + first(N)).\alpha\} - \{m.\alpha\}$ therefore $0 < \{(i-m).\alpha\} < \{first(N).\alpha\}$ which contradicts the definition of first, since $(i-m) \in$ Circle because $0 < i - m < N$.

- if $i \leq m$ then $\{(m + first(N)).\alpha\} - \{i.\alpha\} < \{(m + first(N)).\alpha\} - \{m.\alpha\}$ therefore $\{(m + first(N) - i).\alpha\} < \{first(N).\alpha\}$ which contradicts the definition of first(N), since $(m + first(N) - i) \in$ Circle because $0 < m + first(N) - i < N$.

In these two former cases $\{(m + first(N)).\alpha\} - \{m.\alpha\} = \{first(N).\alpha\}$ if $\{m.\alpha\} < \{(m + first(N)).\alpha\}$.
Let us show this by reductio ad absurdum:
if $\{(m + first(N)).\alpha\} \leq \{m.\alpha\}$ then
$\{(m + first(N)).\alpha\} - \{first(N).\alpha\} \leq \{m.\alpha\} - \{first(N).\alpha\}$
therefore by definition of $first$ $\{m.\alpha\} \leq \{m.\alpha\} - \{first(N).\alpha\}$ which is absurd because $\{first(N).\alpha\} > 0$ for $N \geq 2$.

2. Case $last(N) \leq m < N$:
For $m = last(N)$, by definition of $last$ we have $after(N, last(N)) = 0$.

We want to prove that $m - last(N)$ is the successor of m.
Let us first show that $m - last(N)$ belongs to the circle of N points: if $last(N) < m < N$ then
$0 \leq last(N) - last(N) < m - last(N) < N - last(N) < N$ because $last(N) > 0$.

Now, let us show that: if i any point of the circle $(0 < i < N)$ then we have either $\{i.\alpha\} < \{m.\alpha\}$ or $\{i.\alpha\} > \{(m - last(N)).\alpha\}$.
By reductio ad absurdum and by cases:
let us suppose that $\{m.\alpha\} < \{i.\alpha\} < \{(m - last(N)).\alpha\}$

- if $i < m$ then $\{m.\alpha\} - \{i.\alpha\} + 1 > \{m.\alpha\} - \{(m - last(N)).\alpha\} + 1$ therefore $\{(m - i).\alpha\} > \{last(N).\alpha\}$ which contradicts the definition of last, since $(m - i) \in$ Circle because $0 < m - i < N$.

- if $m \leq i$ then
$\{m.\alpha\} - \{(m - last(N)).\alpha\} + 1 < \{i.\alpha\} - \{(m - last(N)).\alpha\} + 1$
therefore $\{last(N).\alpha\} < \{(i + m - last(N)).\alpha\}$
which contradicts the definition of last, since $(i + m - last(N)) \in$ Circle because $0 < i + m - last(N) < N$.

In these two former cases $\{m.\alpha\} - \{(m - last(N)).\alpha\} + 1 = \{last(N).\alpha\}$ if $\{m.\alpha\} < \{(m - last(N)).\alpha\}$.
As α is irrationnal and by definition of $last$ we have $\{m.\alpha\} < \{last(N).\alpha\}$ therefore $\{(m - last(N)).\alpha\} = \{m.\alpha\} - \{last(N).\alpha\} + 1$ and we have effectively $\{m.\alpha\} < \{m.\alpha\} - \{last(N).\alpha\} + 1$, since $\{last(N).\alpha\} < 1$.

Remark 3. The fact of α is irrational is essential for showing that $\{m.\alpha\} \neq \{last(N).\alpha\}$. Indeed, as in this case we have $m \neq last(N)$ therefore $\{m.\alpha\} \neq \{last(N).\alpha\}$. Let us show this by contradiction.
In order to do so, let us suppose $\{m.\alpha\} = \{last(N).\alpha\}$.
Then $\{m.\alpha\} - \{last(N).\alpha\} = 0$ therefore $\{(m - last(N)).\alpha\} = 0$ and as only an integer number has a fractional part equal to zero we have $(m - last(N)).\alpha = k$, $k \in \mathbb{N}$ from which we conclude that $\alpha = \frac{k}{m - last(N)}$ which contradicts α irrationnal.

$\square$

Let us prove now the general case.
Let us set for the rest of the proof $M = first(N) + last(N)$.

Lemma 5 (Relationship between N and M). $N \leq M$.

Proof.
By reductio ad absurdum. We suppose $M < N$ and we show that, in this case, the point $first(N) + last(N)$ is situated either before $first$, or after $last$, which contradicts their definition.
Let us show, therefore, that either $\{(first(N) + last(N)).\alpha\} < \{first(N).\alpha\}$ or $\{(first(N) + last(N)).\alpha\} > \{last(N).\alpha\}$:
Let us consider the following cases:

1. $\{first(N).\alpha\} + \{last(N).\alpha\} < 1$:
   since for $N \geq 2$ $\{first(N).\alpha\} > 0$ we can write that
   $\{first(N).\alpha\} + \{last(N).\alpha\} > \{last(N).\alpha\}$ thus that
   $\{(first(N) + last(N)).\alpha\} > \{last(N).\alpha\}$.
2. $\{first(N).\alpha\} + \{last(N).\alpha\} \geq 1$:
   in the same way we can write, using the fact that $0 \leq \{\} < 1$, that $\{first(N).\alpha\} + \{last(N).\alpha\} - 1 < \{first(N).\alpha\}$ thus that
   $\{(first(N) + last(N)).\alpha\} < \{first(N).\alpha\}$.

$\square$

Lemma 6. $first(N) = first(M)$.

Proof.
By definition of $first$, we know that for all a and b s.t. $0 < a < N$ and $0 < b < N$ we have that if $\{a.\alpha\} \leq \{b.\alpha\}$ then $a = (first(N))$.
Let us take $N = M$ and $a = (first(N))$ and then we have for all b s.t. $0 < b < M$ if $\{(first(N)).\alpha\} \leq \{b.\alpha\}$ then $(first(N)) = (first(M))$.
Now, it is sufficient to show that $\{(first(N)).\alpha\} \leq \{b.\alpha\}$ $\forall b$, $0 < b < M$:
For $0 < b < N$ it is the definition of $first$ (lemma 1).
For $N \leq b < M$ by the reductio ad absurdum: let us suppose that $\{b.\alpha\} < \{(first(N)).\alpha\}$
As $b < M = first(N) + last(N)$ we have immediately that
$b - first(N) < last(N) < N$ and $b - last(N) < first(N) < N$

and by definition of $first$ and $last$ that $\{(b - first(N)).\alpha\} \leq \{last(N).\alpha\}$ and $\{first(N).\alpha\} \leq \{(b - last(N)).\alpha\}$.
Therefore we have, owing to the hypothesis of contradiction and to lemmas 1 and 2 that:
$\{b.\alpha\} - \{first(N).\alpha\} + 1 \leq \{last(N).\alpha\}$ and
$\{first(N).\alpha\} \leq \{b.\alpha\} - \{last(N).\alpha\} + 1$ which implies that
$\{last(N).\alpha\} + \{first(N).\alpha\} - \{b.\alpha\} - 1 = 0$ thus that
$\{(b - first(N)).\alpha\} = \{last(N).\alpha\}$. But, as shown in Remark 3 this equality compels α to be rational if $b - first(N) \neq last(N)$ which is the case.

$\square$

Lemma 7. *$last(N) = last(M)$.*

Proof.
Symmetrical proof with the previous.

$\square$

Lemma 8. *For all n s.t. $0 < n < N - first(N)$ and $last(N) < n < N$ we have $after(N, n) = after(M, n)$.*

Proof.
We proceed by cases:

1. Case $0 < n < N - first(N)$:
   Using the irrationality of α (counterpart of remark 3) we have that to prove this lemma is equivalent to $\{after(N, n).\alpha\} = \{after(M, n).\alpha\}$ which is also equivalent to
   $\{after(N, n).\alpha\} \leq \{after(M, n).\alpha\}$ and $\{after(M, n).\alpha\} \leq \{after(N, n).\alpha\}$.
   Let us proceed by cases and by reductio ad absurdum:
   - Case $\{after(N, n).\alpha\} \leq \{after(M, n).\alpha\}$:
     Let us suppose that $\{after(N, n).\alpha\} > \{after(M, n).\alpha\}$.
     According to lemma 3, we show immediately the following property:
     $\forall N \in \mathbb{N}, \forall n, k \in Circle$, if $\{n.\alpha\} < \{k.\alpha\}$ and if $\{k.\alpha\} \neq \{after(N, n).\alpha\}$ then $\{after(N, n).\alpha\} < \{k.\alpha\}$. Let us use this property with $k = after(M, n)$. We directly get the contradiction on condition that :
     - $n \in Circle$ i.e. $0 < n < N$; true by case 1.
     - $after(M, n) \in Circle$ i.e. $0 < after(M, n) < N$ true using lemma 4.
     - $\{n.\alpha\} < \{after(M, n).\alpha\}$ by definition of after (lemma 3 and definition 1) + lemma 4 (in order to show that $after(M, n) \neq 0$).
     - $\{after(M, n).\alpha\} \neq \{after(N, n).\alpha\}$ true by hypothesis of contradiction.
   - Case $\{after(M, n).\alpha\} \leq \{after(N, n).\alpha\}$:
     Let us suppose that $\{after(M, n).\alpha\} > \{after(N, n).\alpha\}$. We use the same property taking $k = after(N, n)$ and $N = M$ (except in k).
2. Case $last(N) < n < N$: the proof is done with the same way.

$\square$

For n situated in the third gap, the value of $after(N, n)$ is given from the following lemma :

Lemma 9. *For all n, $N - first(N) \leq n < last(N)$ there does not exist $k \in Circle$ s.t. $\{n.\alpha\} < \{k.\alpha\} < \{(n + first(N) - last(N)).\alpha\}$.*

Proof.
Reduction ad absurdum.
Let us suppose there exists one $k \in Circle$ s.t.
$\{n.\alpha\} < \{k.\alpha\} < \{(n + first(N) - last(N)).\alpha\}$.
This k verifies one of the three following cases (total order on the real numbers):

1. if $\{k.\alpha\} < \{after(M.n).\alpha\}$:
   then $\{n.\alpha\} < \{k.\alpha\} < \{after(M.n).\alpha\}$ which contradicts the definition of the function $after$.
2. if $\{k.\alpha\} = \{after(M.n).\alpha\}$:
   according to lemmas 4 and 6 $after(M, n) = n + first(N)$. But, as α is irrationnal, we ought to have $k = n + first(N)$ which contradicts the hypothesises $n < last(N)$ and $k < N$ (using lemma 5).
3. if $\{k.\alpha\} > \{after(M.n).\alpha\}$:
   we use the already seen property $\forall N \in \mathbb{N}, \forall j, k \in Circle$, if $\{j.\alpha\} < \{k.\alpha\}$ and if $\{k.\alpha\} \neq \{after(N, j).\alpha\}$ then $\{after(N, j).\alpha\} < \{k.\alpha\}$ with $N = M$, $j = n + first(N)$.
   Then we have, using principally lemma 4 that
   $\{(n + first(N) - last(N)).\alpha\} < \{k.\alpha\}$ which contradicts the hypothesis.

$\square$

Proof of theorem 2

Let us suppose that the circle includes M points. Then, we know how to show the theorem (lemma 4). Now, It is sufficient "to remove" the $M - N$ points which are too many.

1. if $0 \leq n < N - first(N)$ then:
   according to lemma 5 we have $0 \leq n < N - first(N) < last(N)$. Using lemmas 6, 7, 8 and 4 we immediately get the result.
2. if $N - first(N) \leq n < last(N)$ then:
   using lemma 9,we show that the $M - N$ points from N do not exist and by definition of $after$ (lemma 3 and definition 1) we get the result.
3. if $last \leq n < N$ then:
   as in case 1.

$\square$

Conclusion

The proof given in this paper has been developped from a proof completely formalized in the system Coq [BB+97].

The advantages of a formal proof

With a mathematical theorem such as this, the interest is twofold: the first consists in indicating the possible limits of the proof assistance system in order to improve it; second, is the emphasizing the basic mathematical properties or hypotheses used implicitly during the demonstration.
This proof is based on geometrical intuitions and the demostration of these intuitions often requires, for example, basic notions about the fractional parts. Even so, these notions are neither easy to formalize nor to prove in a system where real numbers are not naturally found, unlike other types which can be easily defined inductively. So, one challenge was to prove this theorem from a simple axiomatization of the real numbers. The formulation of real numbers used for this will be discussed further.

Throughout this work, we confirmed that the Coq proof assistant system allows us to work out some purely mathematical proofs. For more details, see [MAY99].

Moreover, it is interesting to notice that the theorem shown is, in some sence, stronger than that which was stated initially. Indeed, not only do we show that there are at most three different lengths of gaps, but we can also give their value and their place on the circle. This modified statement is due to [RAV88].

From the proof completely formalized in Coq, we can, for instance, compare this informal proof resulting from the formal proof with that of Tony van Ravenstein.

Properties about $\mathbb{R}$

- Two possibilities exist to describe the real numbers: we can construct the reals or axiomatize them. We chose an axiomatical development for reasons of simplicity and rapidity. We can refer to [LAN71] and [LAN51] for constructions from Cauchy's sequences or Dedekind's cuts. Most properties of the real numbers (commutative field, order, the Archimedian axiom) are first order properties. On the other hand, the completeness property is a second order property, as it requieres to quantify on the sets of real numbers. Instead of this axiom, we can put an infinity of first order axioms, according to which any odd degree has a root in $\mathbb{R}$. Hence, we get the "real closed field" notion. We thus chose axiomatization at the *second order* based on the fact that $\mathbb{R}$ is a **commutative ordered Archimedian and complete field**. For these notions, we based our work on [DIE68] and [HAR96].
- The formal proof showed us that the axiom of completeness of the real numbers was not necessary. Therefore, the statement and the proof of this theorem are true in all the commutative ordered and Archimedean fields.
  Archimedes' axiom could also be replaced by a weaker axiom making it possible to define only the fractional part.
  In the same way, E.Fried and V.T.Sos have given a generalization of this theorem for groups [FR+92].

The fractional parts.

Many intermediate lemmas had to be proved. The formal proof, for instance, made it possible to identify four lemmas concerning the fractional part, which had remained implicit in Tony van Ravenstein's proof, and are at the heart of the proof.

- if $\{r1\} + \{r2\} \geq 1$ then $\{r1 + r2\} = \{r1\} + \{r2\} - 1$
- if $\{r1\} + \{r2\} < 1$ then $\{r1 + r2\} = \{r1\} + \{r2\}$
- if $\{r1\} \geq \{r2\}$ then $\{r1 - r2\} = \{r1\} - \{r2\}$
- if $\{r1\} < \{r2\}$ then $\{r1 - r2\} = \{r1\} - \{r2\} + 1$

Degenerated cases.

The formal proof makes it possible to separate the degenerated cases such that $N = 0$, $N = 1$ and α rational, which can be passed over in silence during an informal proof.

α irrational.

α irrational is hypothesis used by Tony van Ravenstein, but the formalization shows precisely where this hypothesis is used (cf remark 3). In particular, if α is rational, the points can be mingled, and $after$, for example, is not then a function.

first(N) and first(M), last, after.

During Tony van Ravenstein's informal proof, we see that we can tolerate an inaccuracy in the dependence of $first$, $last$ and $after$ to N or M. Although this is not a mistake, the formal proof showed the necessity of proving these lemmas, which are not trivial (lemmas 6, 7 and 8). The formal proof makes it possible to say precisely where those lemmas are used.

Use of the classical logic.

The formal proof carried out in the system Coq - from the axiomatization of real numbers as a commutative, ordered, archimedian and complet field - is a classical proof seeing that an intuitionist reading of the total order involves the decidability of the equality of the real numbers, which obviously, is not the case. Therefore, we can raise the question of the existence of a constructive proof of the three gap theorem.
We could probably give an intuitionistic proof for each of the two cases, according to whether α is rational or irrational because we know exactly the length of the gaps between two points of the circle. But, the two cases cannot be treated at the same time. Thus in our proof it should be supposed that α is rational or not and we do not see, so far how to avoid this distinction.

References

[BB+97] Barras Bruno and al. *The Coq Proof Assistance Reference Manual Version 6.3.1.* INRIA-Rocquencourt, May 2000.
http://coq.inria.fr/doc-eng.html

[DIE68] Dieudonné Jean *Eléments d'analyse. Vol. 1. Fondements de l'analyse moderne.* Gauthier-Villars Paris (1968)

[FR+92] Fried E. and Sós V.T. *A generalization of the three-diatance theorem for groups.* Algebra Universalis 29 (1992), 136-149

[HAL65] Halton J.H. *The distribution of the sequence* $\{\eta\xi\}$ $(n = 0, 1, 2, ...)$. Proc. Cambridge Phil. Soc. 71 (1965), 665-670

[HAR96] Harrison John Robert. *Theorem Proving with the Real Numbers.* Technical Report number 408, University of Cambridge Computer Laboratory, December 1996.

[LAN51] Landau Edmund *Foundations of analysis. The arithmetic of whole, rational, irrational and complex numbers.* Chelsea Publishing Company (1951)

[LAN71] Lang Serge *Algebra.* Addison-Wesley Publishing Company (1971)

[MAY99] Mayero Micaela *The Three Gap Theorem: Specification and Proof in* Coq. Research Report 3848, INRIA, December 1999.
ftp://ftp.inria.fr/INRIA/publication/publi-ps-gz/RR/RR-3848.ps.gz

[RAV88] Van Ravenstein Tony *The three gap theorem (Steinhaus conjecture).* J. Austral. Math. Soc. (Series A) 45 (1988), 360-370

[SLA67] Slater N.B. *Gap and steps for the sequence* $\eta\theta$ *mod 1.* Proc. Cambridge Phil. Soc. 73 (1967), 1115-1122

[SOS57] Sós V.T. *On the theory of diophantine approximations.* Acta Math. Acad. Sci. Hungar. 8 (1957), 461-472

[SOS58] Sós V.T. *On the distribution mod 1 of the sequence* $\eta\alpha$. Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 1 (1958), 127-134

[SWI58] Świerckowski S. *On successive settings of an arc on the circumference of a circle.* Fund. Math. 48 (1958), 187-189

[SUR58] Surányi J. *Über der Anordnung der Vielfachen einer reelen Zahl mod 1.* Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 1 (1958), 107-111