S-structure of Euclidean Algorithm

by Tetsuya NAGANO

Abstract
The purpose of the present paper is to give the standpoint of geometry to Euclidean Algorithm. Euclidean Algorithm is well known to the public. The author gives the new view to Euclidean Algorithm by the theory of the structure of sequences developed by the author 12 years ago.

Keywords: Euclidean Algorithm, S-structure, sequence, hyperbolic curve.

Introduction
The author studied the S-structure of a sequence of numbers[3,4,5]. In [3], Arithmetic and geometric sequences were studied in detail and sequences defined by a difference equation with three terms were classified in three types on 2-dimensional Euclidean space. In [4], sequences defined by a difference equation with four terms were classified in four types on 3-dimensional Euclidean space. In [5], the author treated more general sequences, which aren't expressed uniform as some difference equation. In there, the sub sequences of the original sequence were studied and the local S-structure was defined. The S-structure and local S-structure are the object with the geometrical meaning.

In the first section, the general theory of S-structure of 2-dimensionable sequences is expressed. In the second section, Euclidean Algorithm is stated and in the final section the geometrical objects, it is a hyperbolic curve, corresponding to Euclidean Algorithm are expressed.

1 S-structure of 2-dimensionable sequences

We are given the notion of S-structure of it by [3]. Let $A = \{a_n\}$ be a 2-dimensionable sequence of numbers. We considered the map $l_A : n \longrightarrow$ a line $l_A(n) : a_{n+2} = a_{n+1}x + a_n y$. Then we defined

Definition 1.1 *The set*

$$(1.1) \qquad \bigcap_n l_A(n)$$

is called S-structure of the sequence A.

Further we defined the local S-structure of a sequence A as follows:

Let (x_n, y_n) be the intersection point of lines $l_A(n)$ and $l_A(n+1)$. This point is the S-structure of the sub sequence $a_n,\ a_{n+1},\ a_{n+2},\ a_{n+3}$. We call it the *sub S-structure* of it. Then we define

Definition 1.2 *The set*

$$\bigcup_n (x_n, y_n) \tag{1.2}$$

is called (2-dimensional) local S-structure of the sequence A.

Well, let $A = \{a_n\}$ be a 2-dimensionable sequence defined by a difference equation $a_{n+2} = x_0 a_{n+1} + y_0 a_n$ with real constants x_0, y_0. Then it is clearly true that $(x_n, y_n) = (x_0, y_0)$ for all n. Therefore the 2-dimensional local S-structure of A is a single point (x_0, y_0) from (1.2). According to [5], sequences defined by the above difference equation are characterized two types with respect to the S-structure. One is the type that S-structure is a single point (x_0, y_0), but the other is the type that S-structure is a line of the form $r^2 = rx + y$. And sequences that S-structure is a line are only geometric ones. Thus we have

Proposition 1.1 *Let $A = \{a_n\}$ be a 2-dimensionable sequence defined by a difference equation $a_{n+2} = x_0 a_{n+1} + y_0 a_n$ with real constants x_0, y_0. Then the S-structure of A coincides with the local S-structure of itself, namely,*

$$\bigcap_n l_A(n) = \bigcup_n (x_n, y_n) = (x_0, y_0).$$

Now, we shall express the sub S-structure by its term. The sub S-structure (x_n, y_n) is the intersection point of lines $l_A(n)$ and $l_A(n+1)$, and so it is the solution of the following simultaneous linear equation

$$\begin{cases} a_{n+1}x + a_n y = a_{n+2} \\ a_{n+2}x + a_{n+1}y = a_{n+3}. \end{cases} \tag{1.3}$$

Since the sequence A is the 2-dimensionable one, the equation

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} \dfrac{a_{n+1}a_{n+2} - a_n a_{n+3}}{a_{n+1}^2 - a_n a_{n+2}} \\ \dfrac{a_{n+1}a_{n+3} - a_{n+2}^2}{a_{n+1}^2 - a_n a_{n+2}} \end{pmatrix} \tag{1.4}$$

is satisfied.

On the other hand, since the sub S-structure (x_{n+1}, y_{n+1}) is the intersection point of $l_A(n+1)$ and $l_A(n+2)$, for three terms $a_{n+1}, a_{n+2}, a_{n+3}$ the following simultaneous linear equation

$$\begin{cases} x_n a_{n+2} + y_n a_{n+1} = a_{n+3} \\ x_{n+1} a_{n+2} + y_{n+1} a_{n+1} = a_{n+3} \end{cases} \tag{1.5}$$

is satisfied. Therefore the following equation

$$(1.6) \qquad (x_{n+1}-x_n)a_{n+2}+(y_{n+1}-y_n)a_{n+1}=0$$

is satisfied. Thus we have

Theorem 1.1 *Let $A=\{a_n\}$ be a 2-dimensionable sequence. Then the sub S-structure of A is written in the form (1.4) and the binomial equation (1.6) is also satisfied for all n.*

Here we put

$$(1.7) \qquad D(n)=x_{n+1}y_n-x_ny_{n+1}.$$

If $D(n)=0$, the proportional relation $x_n:y_n=x_{n+1}:y_{n+1}$ is satisfied. Therefore if $(x_n,y_n)\neq(x_{n+1},y_{n+1})$ is satisfied, the line $l_A(n+1)$ passes the origin. Namely, $a_{n+3}=0$ is satisfied.

If, for all n, $D(n)=0$ and $(x_n,y_n)\neq(x_{n+1},y_{n+1})$ are satisfied, then $a_{n+3}=0$ is also satisfied for all n. But the sequence A is 2-dimensionable so that $a_{n+3}=0$ $(n\geq 1)$ is contradictory. Thus we have

Proposition 1.2 *Let $A=\{a_n\}$ be a 2-dimensionable sequence. If $D(n)=0$ is satisfied for all n, then its all sub S-structures are the same intersection point, namely, its local S-structure is a singleton.*

Here we denoted the intersection point of Proposition 1.2 by (x_0,y_0). Then we have, from Proposition 1.1 and 1.2,

Theorem 1.2 *A 2-dimensionable sequence $A=\{a_n\}$ is defined by the difference equation $a_{n+2}=x_0a_{n+1}+y_0a_n$ with real constants x_0,y_0, if and only if $D(n)=0$ is satisfied for all n. Then (x_0,y_0) is the local S-structure of A.*

Next, if $D(n)\neq 0$ is satisfied, then from (1.5), the equation

$$(1.8) \qquad a_{n+1}=\frac{x_{n+1}-x_n}{x_{n+1}y_n-x_ny_{n+1}}a_{n+3} \quad \text{and} \quad a_{n+2}=\frac{y_n-y_{n+1}}{x_{n+1}y_n-x_ny_{n+1}}a_{n+3}$$

are satisfied. Therefore we have

Proposition 1.3 *Let $A=\{a_n\}$ be a 2-dimensionable sequence. If $D(n)\neq 0$ is satisfied for all n, then (1.8) is satisfied with respect to three terms a_{n+1},a_{n+2},a_{n+3}.*

Lastly, we apply (1.8) to x_n or y_n of (1.4), and we have

$$(1.9) \qquad a_n=\frac{y_n-y_{n+1}+x_n^2-x_nx_{n+1}}{(x_{n+1}y_n-x_ny_{n+1})y_n}a_{n+3},$$

where $y_n\neq 0$.

2 Euclidean Algorithm

We know *Euclidean Algorithm.* It is dependent on the following theorem.

Theorem 2.1 *Let $a, b(0 < a \leq b)$ be arbitrary integers. Then there exist integers q and r, uniquely, satisfying the following equation*

$$b = qa + r \ (0 \leq r < a).$$

To obtain the greatest common divisor(G.C.D.) of a, b we can apply the theorem to the quotient q and the remainder r, and we have the following system of the quotients and remainders

$$\begin{aligned} b &= q_1 a + r_1 \quad (0 \leq r_1 < a) \\ a &= q_2 r_1 + r_2 \quad (0 \leq r_2 < r_1) \\ r_1 &= q_3 r_2 + r_3 \quad (0 \leq r_3 < r_2) \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \quad (0 \leq r_n < r_{n-1}) \\ r_{n-1} &= q_{n+1} r_n + r_{n+1} \quad (r_{n+1} = 0). \end{aligned}$$

This series $b \geq a > r_1 > r_2 > \cdots > r_{n-1} > r_n > r_{n+1} = 0$ is the monotone decreasing sequence. In this time, r_n is the G.C.D. of a and b.

In the next section, we consider the S-structure of the above sequence $b, a, r_1, \cdots, r_n, 0$. Hereafter, we call this sequence *Euclidean algorithm.*

3 S-structure of Euclidean Algorithm

We want to study about the S-structure of the above sequence "Euclidean algorithm".

First, we assume that integers a and b $(a \leq b)$ satisfy the equation

(3.1) $$b = qa + 1.$$

In this time, we have the sequence as Euclidean algorithm

(3.2) $$b, a, 1, 0$$

and these integers a, b are *relatively prime*, namely, $gcd(a, b) = 1$.

From (1.4), its S-structure (x, y) is

(3.3) $$(x, y) = \left(\frac{-a}{b - a^2}, \frac{1}{b - a^2} \right),$$

where $b - a^2 \neq 0$ because that if $b - a^2 = 0$, from (3.1), the equations $a^2 = qa + 1$ and $q = a - \frac{1}{a}$ are satisfied. However, a is an integer so that q is not integer. This is incorrect.

Now we shall study the S-structure (3.3). We see $y \neq 0$, therefore we have

$$(3.4) \qquad \begin{cases} b = \dfrac{1}{y} + \dfrac{x^2}{y^2} \\ a = -\dfrac{x}{y} \end{cases}$$

From (3.1) and (3.4), we have

$$(3.5) \qquad \frac{1}{y} + \frac{x^2}{y^2} = -q\frac{x}{y} + 1.$$

Therefore the equation

$$(3.6) \qquad x^2 - y^2 + qxy + y = 0 \quad (q : \text{a positive integer})$$

holds good.

Conversely, if the S-structure (3.3) of a sequence $b, a, 1, 0 (a \leq b)$ is on the hyperbolic curve (3.6) in Euclidean Space R^2, then $b = qa + 1$ (q : a positive integer) is satisfied. Therefore the sequence $b, a, 1, 0 (a \leq b)$ is Euclidean algorithm. Thus we have

Theorem 3.1 *A sequence $b, a, 1, 0 (a \leq b)$ is Euclidean algorithm if and only if its S-structure is on the hyperbolic curve (3.6) in Euclidean Space R^2.*

Next we consider the case that the sequence

$$c, b, a, 0 \ (c \geq b \geq a > 0)$$

is Euclidean algorithm. Then

$$(3.7) \qquad c = q_1 b + a \qquad (q_1 : \text{a positive integer})$$

and

$$(3.8) \qquad b = q_2 a \qquad (q_2 : \text{a positive integer})$$

are satisfied. This means that $gcd(b, c) = a$.
In this case, its S-structure (x, y) is, from (1.4)

$$(3.9) \qquad (x, y) = \left(\frac{-ab}{ca - b^2}, \frac{a^2}{ca - b^2}\right).$$

However, from (3.7) and (3.8), we have

$$(3.10) \qquad (x, y) = \left(\frac{-ab}{ca - b^2}, \frac{a^2}{ca - b^2}\right) = \left(\frac{-q_2}{q_1 q_2 + 1 - q_1^2}, \frac{1}{q_1 q_2 + 1 - q_1^2}\right).$$

This sequence has the same S-structure as the sequence $q_1q_2+1, q_2, 1, 0$ has. Therefore the S-structure (3.9) is on the hyperbolic curve

$$x^2 - y^2 + q_1xy + y = 0. \tag{3.11}$$

Thus, from Theorem 3.1 we have

Theorem 3.2 *The sequence $c, b, a, 0$ $(c \geq b \geq a > 0)$ is Euclidean algorithm if and only if the S-structure (3.9) is on the hyperbolic curve (3.11).*

Lastly, we treat the case that the sequence $c, b, a, 1, 0$ $(c \geq b \geq a \geq 1)$ is Euclidean algorithm. This sequence satisfies

$$c = q_1b + a \quad \text{and} \quad b = q_2a + 1 \ (q_1, q_2 : \text{positive integers}). \tag{3.12}$$

In this case, $gcd(b, c) = 1$.

We will consider the local S-structure of it because that, in general, S-structure is null set in this case. The local S-structure is the solution of the following system

$$(\mathrm{I})\begin{cases} a = bx + cy \\ 1 = ax + by \end{cases} \quad \text{and} \quad (\mathrm{II})\begin{cases} 1 = ax + by \\ 0 = x + ay \end{cases}. \tag{3.13}$$

We have the solution

$$(\mathrm{I})\left(\frac{ab-c}{b^2-ca}, \frac{b-a^2}{b^2-ca}\right) \quad \text{and} \quad (\mathrm{II})\left(\frac{-a}{b-a^2}, \frac{1}{b-a^2}\right). \tag{3.14}$$

From (3.14)-(II) and Theorem 3.1, the sub S-structure of the sub sequence $b, a, 1, 0$ is on the hyperbolic curve

$$x^2 - y^2 + q_2xy + y = 0. \tag{3.15}$$

We will study the sub S-structure (3.14)-(I). We put

$$x = \frac{ab-c}{b^2-ca}, \quad y = \frac{b-a^2}{b^2-ca}. \tag{3.16}$$

Since the equation $b \neq 0$ is true, we put $t = \frac{a}{b}$ and the following system from (3.12)

$$\frac{c}{b} = q_1 + t \quad \text{and} \quad 1 = q_2t + \frac{1}{b} \tag{3.17}$$

holds good. Further from the first equation of (3.16),

$$x = \frac{\frac{a}{b} - \frac{c}{b^2}}{1 - \frac{c}{b}\frac{a}{b}} = \frac{t - \frac{c}{b}\frac{1}{b}}{1 - \frac{c}{b}t} \tag{3.18}$$

is satisfied. From (3.17) and (3.18), we have

$$x = \frac{-q_2t^2 - q_1q_2t + q_1}{t^2 + q_1t - 1}. \tag{3.19}$$

From the same manner, we have

$$y = \frac{t^2 + q_2t - 1}{t^2 + q_1t - 1}. \tag{3.20}$$

From (3.19) and (3.20), the equations

$$(x + q_2)t^2 + q_1(x + q_2)t - (x + q_1) = 0 \tag{3.21}$$

and

$$(y - 1)t^2 + (q_1y - q_2)t - (y - 1) = 0 \tag{3.22}$$

are satisfied.
Next, from (3.22) $\times$ $(x + q_2)$ $-$ (3.21) $\times$ $(y - 1)$, we have

$$(x + q_2)(q_1 - q_2)t + (y - 1)(q_1 - q_2) = 0. \tag{3.23}$$

Therefore the equation

$$t = \frac{1 - y}{x + q_2} \tag{3.24}$$

is satisfied.
Finally, from (3.21)(or (3.22)) and (3.24), we have the hyperbolic curve

$$x^2 - y^2 + q_1xy + (2 + q_1q_2)y + q_2x - 1 = 0. \tag{3.25}$$

The converse is also true. Thus we have the following theorem

Theorem 3.3 *The sequence $c, b, a, 1, 0$ $(c \geq b \geq a \geq 1)$ is Euclidean algorithm if and only if its local S-structure (3.14) satisfies as follows:*
(1) its sub S-structure of sub sequence $b, a, 1, 0$ is on the hyperbolic curve (3.15), where $b = q_2a + 1$.
(2) its sub S-structure of sub sequence $c, b, a, 1$ is on the hyperbolic curve (3.25), where $c = q_1b + a$.

Moreover, for the sequence $d, c, b, a, 0$, its sub S-structure of sub sequence $c, b, a, 0$ is

$$\left(\frac{-ab}{ca - b^2}, \frac{a^2}{ca - b^2}\right), \tag{3.26}$$

and its sub S-structure of sub sequence d, c, b, a is

$$\left(\frac{bc - ad}{c^2 - bd}, \frac{-b^2 + ca}{c^2 - bd}\right). \tag{3.27}$$

In this time, from the same reason for Theorem (3.2), we have the following theorem

Theorem 3.4 *The sequence* $d, c, b, a, 0$ $(d \geq c \geq b \geq a)$ *is Euclidean algorithm if and only if its local S-structure satisfies as follows:*
(1) its sub S-structure (3.26) of sub sequence $c, b, a, 0$ *is on the hyperbolic curve (3.15), where* $c = q_2 b + a$.
(2) its sub S-structure (3.27) of sub sequence d, c, b, a *is on the hyperbolic curve (3.25), where* $d = q_1 c + b$.

4 References

[1] R. Bronson: Linear Algebra, 87-162, Academic Press, U.S.A., 1995.

[2] J. Gilbert and L. Gilbert: Linear Algebra and Matrix Theory, 113-127, ibid., 1995.

[3] T. Nagano: On S-structure(I), *J.Nagasaki Pref. Women's Jr. Coll.* 42, 1-7(1994).

[4] T. Nagano: On S-structure(II), ibid.,43, 1-9(1995).

[5] T. Nagano: On two-dimensionable sequences, ibid., 44, 1-9(1996).

[6] H. Suda: Difference Equation · Differential Equation(Japanese), 33-48, Baifukan, Tokyo, 1983.