Pratiques algorithmiques dans les mathématiques pré-modernes
Symposium du projet ALGO (ANR-09-BLAN-0300-01),
organisé par Fabio Acerbi (CNRS, UMR 8163 STL) et Marc Moyon (Université de Limoges).

12-14 octobre 2011, Université de Lille 3 (Villeneuve d'Ascq).

DÉMONTRER LA CORRECTION D'ALGORITHMES PAR LE BIAIS D'ALGORITHMES EN CHINE ANCIENNE

Karine Chemla
REHSEIS—SPHERE UMR 7219
Cnrs & U. Paris Diderot

1. The nature of the statement of the algorithm to be proved in ancient Chinese sources

2. Indicating reasons for the correctness in the statement of an algorithm
—The meaning *yi* and the conditions for its formulation

3. Operating on the statement of an algorithm within the framework of a proof

SOURCES

HANDED DOWN THROUGH THE WRITTEN TRADITION

The Nine Chapters on Mathematical Procedures 九章算術
(abbreviated to ***The Nine Chapters***)

ca. 1st century before/**after** C.E.

Commentaries

Liu Hui 劉徽 (completed in 263)
Li Chunfeng et al. **李淳風** (completed in 656 by a group of scholars under Li)

NB 1 : Canon in capital letters/commentaries in small letters
NB 2 : If no mention, critical edition in Chemla & Guo, *Les neuf chapitres*, Dunod, 2004.

RECENTLY EXCAVATED

Book on mathematical procedures
算數書
from a tomb sealed before *ca* 186 BCE

1. **The nature of the statement of the algorithm to be proved in ancient Chinese sources**

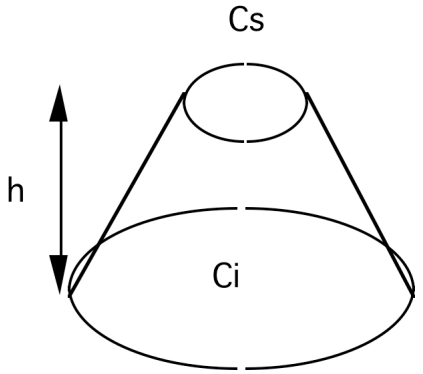
2. Indicating reasons for the correctness in the statement of an algorithm
—The meaning *yi* and the conditions for its formulation

3. Operating on the statement of an algorithm within the framework of a proof

The statement to be proved is most of the time not a single sentence, but a list of operations. It unfolds in time

Example (5.11) "Suppose one has a truncated pyramid with a circular base, the circumference of the lower circle of which is 3 *zhang*, the circumference of the upper circle of which is 2 *zhang*, and the height of which is 1 *zhang*. One asks how much the volume is. Answer: 527 *chi* 7/9 *chi*."

"The circumferences of the upper and lower circles
being multiplied by one another,
then multiplied each by itself,
one adds these (the results);
one multiplies this by the height
and divides by 36."



Multiplications Sum	Multiplication by h	Division by 36
C_i ——————> $C_i\,C_s+C_i^2+C_s^2$	——————> $(C_i\,C_s+C_i^2+C_s^2)h$	——————> $(C_i\,C_s+C_i^2+C_s^2)h/36$
C_s		

The prescription of operations is not always straightforward.

In addition to prescribing by “one multiplies,” “one divides,”
one finds prescriptions grouping several operations: “one makes communicate”

Example (1-17—1.18)

經分

術曰：以人數爲法，錢數爲實，實如法而一。有分者通之； 重有分者同而通之。

DIRECTLY SHARING PROCEDURE:

[1] ONE TAKES THE QUANTITY OF PERSONS AS DIVISOR,

[2] THE QUANTITY OF CASH AS DIVIDEND,

[3] AND ONE DIVIDES THE DIVIDEND BY THE DIVISOR.

[4] IF THERE IS ONE TYPE OF PART, ONE ***MAKES* THEM *COMMUNICATE*.**

[5] IF THERE ARE SEVERAL TYPES OF PARTS,
ONE ***EQUALIZES*** THEM AND HENCE ***MAKES* THEM *COMMUNICATE*.**

DIRECTLY SHARING PROCEDURE:

[1] ONE TAKES THE QUANTITY OF PERSONS AS DIVISOR,

[2] THE QUANTITY OF CASH AS DIVIDEND,

[3] AND ONE DIVIDES THE DIVIDEND BY THE DIVISOR.

[4] IF THERE IS ONE TYPE OF PART, ONE ***MAKES* THEM *COMMUNICATE*.**

[5] IF THERE ARE SEVERAL TYPES OF PARTS,

ONE ***EQUALIZES*** THEM AND HENCE ***MAKES* THEM *COMMUNICATE*.**

Fundamental case — case 1: the data are integers and one divides between integers.

It is **solved by [1], [2], [3]**.

Second case: The data **have one type of fractions.** They can be of the type

either $(a + \frac{b}{c})$ and d, or $(a + \frac{b}{c})$ and $(d + \frac{e}{c})$

[4] "making communicate."

This operation is applied to quantities such as $(a + \frac{b}{c})$ and d or $(d + \frac{e}{c})$.

It transforms $(a + \frac{b}{c})$ into $ac + b$, and either d or $(d + \frac{e}{c})$ into cd (or $cd + e$).

[1], [2], [3]. The procedure is concluded by division

$$(a + \frac{b}{c})/d = (ac + b)/dc \qquad (a + \frac{b}{c})/(d + \frac{e}{c}) = (ac + b)/(dc + e)$$

Third case: The data have **several distinct denominators**.

[5] Case 3 is reduced to the previous one by the operation of "equalizing." Then **([4]), [1], [2], [3].**

$$(a + \frac{b}{c})/(d + \frac{e}{f} + \frac{g}{h}) = (a + \frac{bfh}{cfh})/(d + \frac{ech + gfc}{cfh})$$

The prescription of operations is not always straightforward.

In addition to prescribing by “one multiplies,” “one divides,”
one finds prescriptions grouping several operations: “one makes communicate”

An algorithm *qua* list of operations may cover several cases

The way in which the practitioner uses the text and circulates within the text is not to be taken for granted.

Various ways in which the statement of the algorithm is apprehended in time.

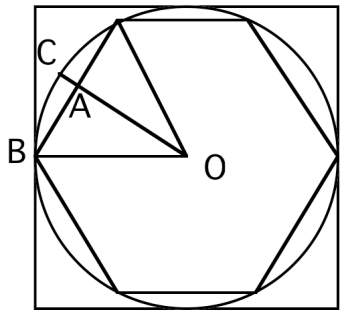
Such are the features of the statements to be proved correct

namely,
to be proved: they **yield** the **required magnitude**, and a **correct value** for it
(value exact or approximate)

1. The nature of the statement of the algorithm to be proved in ancient Chinese sources

2. Indicating reasons for the correctness in the statement of an algorithm
—The meaning *yi* and the conditions for its formulation

3. Operating on the statement of an algorithm within the framework of a proof



割六觚以爲十二觚術曰：置圓徑二尺，半之爲一尺，即圓裏觚之面也。令半徑一尺爲弦，半面五寸爲句，爲之求股。以句冪二十五寸減弦冪，餘七十五寸。開方除之，(…)。故得股八寸六分六釐二秒五忽五分忽之二。以減半徑，餘一寸三分三釐九毫七秒四忽五分忽之三，謂之小句。觚之半面而又謂之小股。爲之求弦。其冪二千六百七十九億四千九百一十九萬三千四百四十五忽，餘分棄 之。開方除之，即十二觚之一面也。”

“Procedure consisting in cutting the 6-gon in order to make a 12-gon: **One sets up the diameter of the circle, 2 *chi*.** One **halves it**, which makes 1 *chi* and gives the side of the 6-gon that is in the circle.

“**One takes half of the diameter,** 1 *chi*, **as hypotenuse**, **half of the side**, 5 *cun*, as **base (of the right-angled triangle)**, and one **looks for the corresponding height**. The **square of the base**, 25 *cun*, being **subtracted from the square of the hypotenuse**, there remains 75 *cun*. One **divides this by extraction of the square root** (…description of the computation of an approximation in the form of a sequence of units concluded by a decimal fraction, in the end simplified…). Consequently, one obtains 8 *cun* 6 *fen* 6 *li* 2 *miao* 5 and two-fifths *hu* for the height.”

“One **subtracts** this (i.e., the height) from the **half-diameter**, 1 *cun* 3 *fen* 3 *li* 9 *hao* 7 *miao* 4 and three-fifths *hu* remains, that one calls small base. **Half** of the polygon side then is **called once again** small height. **One looks for the corresponding hypotenuse**. Its square is 267949193445 *hu*, the remaining fraction being left out. **One extracts the square root,** which gives a side of the 12-gon.

First modality according to which the proof follows/echoes the text of the algorithm

— The algorithm can be interpreted step-by-step, subprocedure by subprocedure until one reaches the final result, which meaning is thereby established. **This is possible since the algorithm is "transparent." I come back later to this property.**

— In the case of the dodecagon, the meaning is established by reference to a diagram (geometrical situation)

— The commentator writes simultaneously the algorithm and its proof. In other cases, the algorithm is stated in *The Nine Chapters,* and the meaning is made explicit in the commentary.

- Part played by problems in the writing of the algorithm & its proof
- The meaning *yi*
- Same kind of algorithm in *Book of mathematical procedures*
- Same kind of algorithm & connection proof/algorithm in al-Khwarizmi's *Algebra*

Second modality according to which the proof follows/echoes the text of the algorithm

— The proof brings into play ideas that echo the terms by which the operations are prescribed.

Back to division between integers increased by fractions

DIRECTLY SHARING PROCEDURE:

[1] ONE TAKES THE QUANTITY OF PERSONS AS DIVISOR,

[2] THE QUANTITY OF CASH AS DIVIDEND,

[3] AND ONE DIVIDES THE DIVIDEND BY THE DIVISOR.

[4] IF THERE IS ONE TYPE OF PART, ONE ***MAKES* THEM *COMMUNICATE*.**

[5] IF THERE ARE SEVERAL TYPES OF PARTS,

ONE ***EQUALIZES*** THEM AND HENCE ***MAKES* THEM *COMMUNICATE*.**

Proof

Third case: The data have **several distinct denominators**.

[5] By "equalizing" the denominators, the third case is reduced to **second case**

Main case: Second case: The data **have one type of fractions.** They can be of the type

either $(a + \frac{b}{c})$ and d, or $(a + \frac{b}{c})$ and $(d + \frac{e}{c})$

[4] "making communicate."

This operation is applied to quantities such as $(a + \frac{b}{c})$ and d or $(d + \frac{e}{c})$.

It ensures that a and b are **made to communicate**," namely, that they share the same units.

It ensures that d and e are **made to communicate**," namely, that they share the same units.

It is applied in parallel to $(a + \frac{b}{c})$ **and** d or $(d + \frac{e}{c})$,

since being dividend and divisor, they **communicate**.

Thus it transforms $(a + \frac{b}{c})$ into $ac + b$, and either d or $(d + \frac{e}{c})$ into cd (or $cd + e$).

Liu Hui reads "Making communicate" as

prescribing the operations at the same time as it indicates the reason for their validity.

[1], [2], [3]. The problem is thus reduced to the first case, and the procedure is concluded by division

$(a + \frac{b}{c})/d = (ac + b)/dc$ $(a + \frac{b}{c})/(d + \frac{e}{c}) = (ac + b)/(dc + e)$

Key idea:

— Liu Hui reads an indication of the reasons underlying the correctness of the algorithm in the terms which prescribe the operations.

— NB: the "**meaning**" is made explicit with respect

- to "**parts**" –one has similar interpretation in *Book of mathematical procedures*

as well as

- **formally**: not to be found in the manuscripts excavated.

Thus two features of the text of an algorithm linked to the proof of the correctness

— **T**he fact that the text has a structure **transparent, namely,** such that the meaning of the successive steps or subprocedures can be interpreted one after the other.

— The terms chosen to prescribe the operations

According to the interpretation of Jens Hoyrup for Mesopotamian clay tablets,

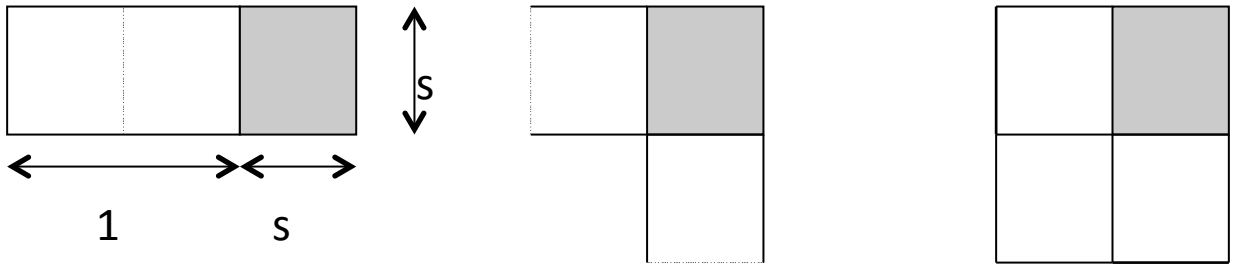
The texts designed to formulate the algorithms make use of the two features simultaneously.

BM 13901 —Mesopotamian text
(Hoyrup, *Lengths, widths, surfaces*, Springer, 2002, p. 11-13**)**

Thureau-Dangin
« J'ai **additionné** la surface et (le côté de) mon carré : 45'.

Tu poseras 1°, l'*unité*. Tu **fractionneras** en deux 1° : 30'. Tu **multiplieras** (entre eux) [30'] et 30' : 15'. Tu **ajouteras** 15' à 45' : 1°. 1° **est le carré de** 1°. 30', que tu as multiplié (avec lui-même), de 1° tu **soustrairas** : 30' est le (côté du) carré. »

Hoyrup
"1. The surface **and** my confrontation: 45' is it. 1, the **projection**,
2. you posit. The **moiety** of 1 you **break**, 30' and 30' you **make hold** each other.
3. 15' to 45' you **append**: by 1, 1 is the equalside. 30' which you have made hold
4. in the inside of 1 you **tear out**: 30' the confrontation



1. The nature of the statement of the algorithm to be proved in ancient Chinese sources

2. **Indicating reasons for the correctness in the statement of an algorithm**
—The meaning *yi* and the conditions for its formulation

3. **Operating on the statement of an algorithm within the framework of a proof**

Why are not all texts for algorithms transparent? The example of the rule of three

(**2.0**) "SUPPOSE
PROCEDURE: ONE MULTIPLIES, BY THE QUANTITY OF WHAT ONE HAS, THE *LÜ* OF WHAT ONE SEEKS, WHAT MAKES THE DIVIDEND; ONE TAKES THE *LÜ* OF WHAT ONE HAS AS DIVISOR. (…commentary) DIVIDING (…)"

quantity of what one has —quantity of what one seeks
***lü* of what one has—*lü* of what one seeks**

Procedure to determine the quantity of what one seeks:
quantity of what one has **times** *lü* of what one seeks **divided by** *lü* of what one has

(…) **(Paradigm—problem) "**If one relies on the fact the the *lü* for foxtail millet is 5 whereas the *lü* for coarsely husked grain is 3, then with 5 of foxtail millet one makes 1 and with 3 of corsely husked grain one makes 1.

If one wants to transform foxtail millet to make coarsely husked, the foxtail millet must first take this 1 (unit) as its base. That it becomes this 1, this means that, simplifying it by 5, one makes that 5 becomes 1. When this is over, then multiplying this (the result) by 3, one makes that 1 becomes 3. In that way, then when the *lü* becomes 1, one takes 5 to make 3."

Transparent procedure established, distinct from the procedure to be established
Liu Hui operates a transformation

"However, if one first divides and then multiplies, there are cases when there are remaining parts, **this is why the procedure inverts the order** (of the operations). "

Procedure first established to yield the desired result

quantity of what one has **divided by** *lü* of what one has **times** *lü* of what one seeks

The procedure is interpreted step-by step, since it is produced step by step

Procedure to be established

quantity of what one has **times** *lü* of what one seeks **divided by** *lü* of what one has

Liu Hui accounts for WHY the two differ
in terms of the ease of computations prized by the authors of the procedure

An operation was applied to the algorithm *qua* list of operations to transform it into another list of operations.

The application of such operations is the cause why some texts of algorithms are not transparent. As far as I can tell, these operations are first attested in Chinese texts.

Liu Hui restores these operations to account for the correctness of an algorithm and its form