IDENTITIES

Enlightening
Interdisciplinarity
in STEM
for Teaching

Tools for designing courses: Elements of the Theory of Didactical Situations (TDS)

Cryptography module

Co-funded by the
Erasmus+ Programme
of the European Union

Grant Agreement n°2019-1-IT02-KA203-063184

The theory of didactical situations (TDS)

A theory and a methodology
for organizing teaching and learning situations

The TDS has been developed by Guy Brousseau at the beginning of the eighties. It relies on some postulates shared by other theories.

Brousseau, G. (1997) Theory of Didactical Situations in Mathematics.
Edited and translated
by Nicolas Balacheff, Martin Cooper, Rosamund Sutherland and Virginia Warfield.
Kluwer Academic Publishers

- It is possible to describe, analyse and explain teaching and learning phenomena in a rational way.
- To achieve this, it is necessary to develop an original theoretical framework, with its specific concepts and methods.
- It is necessary that theory and experimentation be closely related, enriching each other.
- Individuals learn by adapting to a *milieu* that provides contradictions, obstacles, ruptures (link with Piaget's concepts of adaptation and assimilation).

The responsibility of the teacher is to create the conditions favoring the student's learning, while the student is responsible of his/her own learning in a given situation. This corresponds to the concept of ***devolution*** (the process by which the teacher in a didactic situation manage that the student's actions are justified only by the needs of the milieu and its own knowledge, not by didactical means of the teacher).
In this purpose the teacher organise the ***milieu*** in order to provide students the better opportunity to learn. This is related to the process of research of the ***didactical contract*****,** which is specific of the target knowledge. (Brousseau, 1997)

In a didactical situation, the *milieu* is the system that provides retroactions to the student's actions. In case the milieu provides retroactions that allow students to decide by themselves if their actions are successful or not, the situation is said to be ***a-didactical***. It functions as if there were no "didactical intentions" (this is a kind of fiction). The student takes the responsibility of his/her learning (linked to *devolution*).
There are three types of *a-didactical situations*: *action pattern*; *communication pattern*; *explicit validation pattern.*
(Brousseau, 1997, p. 65-72)

Some of the relevant questions in *action patterns*

- Is the *milieu* perceived as devoid of didactical intention?
- Does the student need to choose among several states ?
- Does the student know the final state, or not ?
- Can the student lose and know that he/she can ?
- Can the student be taught the rules without knowing a winning strategy or a solution?
- Is the target knowledge necessary to pass from a basic strategy to a better or (optimum) strategy.
- Is the control of decision possible for the student?

The *didactical contract* is the set of mutual obligations of each partners of the didactical situation, explicit or implicit, for what concerns the knowledge at stake. The usual contract is that the teacher teaches solutions and answers, hence the student does not takes responsibility of his/her learning. A consequence is that the student's learning will not rely on the usual contract, but on its ruptures and ajustements.

Didactical variables

In a situation with an a-didactical dimension, a ***didactical variable*** is a variable with relevant values likely to modify the hierarchy of solving strategies, or to change the optimal strategy of the situation, that have an impact of the target knowledge. For a given mathematical situation, the teacher can make choices linked to his/her teaching objectives among the values of the relevant didactical variables.
Identifying and describing all possible choices is important to understand the meaning of knowledge in the situation

Didactical variables

There are *mathematical (and computer science) didactical variables*, directly linked to the problem at stake.
There are also *organisational didactical variables.*
Choices of both types of variables are contributing to the organisation of the milieu, that comprises also the students' stabilized knowledge likely to be involved in the situation.

The model developed by Guy Brousseau is relevant for the designing of didactical situation, for which conditions offering the best opportunities for learning are determined in a rather precise way.
The problems used for designing such situations are chosen in order to carry the meaning of the target knowledge.
For designing didactical situations for implementation in classroom, it is recommended to chose problems that have already proved to be relevant.

This necessitates at least the following conditions:

1. the student is able to propose an answer based on his/her previous stabilised knowledge, but this first answer is not the target one (otherwise, there is nothing to learn);
2. his/her answer should appear rather quickly as inadequate so that the student need to adapt and modify his/her knowledge.
3. the target knowledge is a priori necessary for providing the correct answer;
4. there is a *milieu* for validation ; the milieu provides relevant retroactions;
5. by choosing values for relevant didactical variables, it is possible to generate different didactical situations relying on this problem.

Didactical Situation based on the Perfect Dominating Set Cryptosystem

Learning objectives

1. Manipulate a public-key cryptosystem based on a computationally hard problem. Students will understand the notions of encryption, decryption, private and public keys.
2. Introduce and explore the notion of one-way-functions.
3. Explore the interdisciplinary nature of one-way-functions, graphs, computational complexity.

Motivations for choosing the TDS (1)

The TDS looks suitable for cryptography, mainly because *deciphering correctly an encrypted message can be easily verified by the students themselves, without calling for the teacher.*

That means that thanks to the *retroaction of the milieu* the action pattern will fit with a-didactical dimension.

Motivations for choosing the TDS (2)

By mixing students with background in mathematics and computer science, *we introduce in the milieu of the situation stabilised knowledge from both domains, that is likely to foster emergence of interdisciplinary strategies*.
In addition, the presence of participants with a background in physics and/or chemistry might favour the introduction of relevant contexts linked with the questions at stake ; by the way, the *milieu* of the situation is enriched.

Relevant features of the chosen problem

- *Plaintext message*: an integer number (88 in our case)
- *Ciphertext message*: the graph with the public values
- *Public key*: the graph (without the PDS)
- *Private key*: the PDS
- *Computationally hard problem* (base of the *one-way function*): it is computationally hard to find the PDS of a graph.

The didactical situation (1)

- *The first step* (common to all subgroups) introduces in the *milieu* shared knowledge (exercice on encryption for all three groups).
- *The second step* is organised considering three values of a crucial didactic variable of the problem.

A crucial didactical variable

V1: “Information provided” (three values)

- *Providing the public key* (the graph) *and the private key* (the perfect dominating set) (Group A)
- *Providing the public key* (the graph) *and the decryption algorithm* (add the numbers on the perfect dominating set) (Group B)
- *Providing only the public key* (the graph without the perfect dominating set) (Group C)

The didactical situation (2)

Step 2 comprises both *action pattern* and (written) *formulation pattern* (preparation of the debate).
The milieu of the didactical situation is different for each group. This has an impact on the possible solving strategies.

Step 3 corresponds to a *validation pattern* (groups' presentation /collective debate on the groups' work)

Other didactical variables

V2 - The decomposition of the number that will be encrypted

V3 - The size of the graph (number of nodes)

V4 - The size of the Perfect Dominating Set (number of nodes in the PDS)

V5 - Connectivity

- V5-A - Presence or absence of leaves (nodes with only one neighbor)
- V5-B - The size of the PDS stars

V6 - The definition of the PDS and the examples.

V7 - Use of computer tools and/or calculators

IDENTITIES

Enlightening
Interdisciplinarity
in STEM
for Teaching

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

UNIVERSITAT DE
BARCELONA

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

UNIVERSITÀ
DI PARMA

Co-funded by the
Erasmus+ Programme
of the European Union

Grant Agreement n°2019-1-IT02-KA203-063184