The problem of the equality

Juan Manuel Dato Ruiz

jumadaru@gmail.com

Abstract

We can find different ways to demonstrate the difference between P and NP. One of them will appear with the connection with the physics, that document is not published yet, but I have some interesting theories about the Sharp-P and a new definition of entropy that will connect the non-functionally requirements with an easy managing of the code. Other way is with an entanglement of data (problem of knowledge). If we merge data and we use it with correspondences, then we will get results with a mathematical impossible return (the strongest functions of one way). If the only one way is by guessing, then NP is different of P.

Explanation.

If we have the intention of demonstrating both classes are different, we have to study the distinction of some kind of problems we can find before. That is, when we generate a correspondence between two datas every knowledge we have about one of them will change the knowledge of the other. That concept is very important, because the existence of a correspondence obligates us to restrict the idea we have about what is exactly an assigment: if we declare a link between two datas then we will have to reject some combinations which never assert the invariant of the system.

Therefore we would define systems where the knowledge of some datas could get us hidding other datas. However we have to construct before that kind of machines in a constructive way, that is, the objective of this document if showing his existence; creating a system which works in that way.

So, before constructing pragmatic applications (digital signature or creation of secure channels from unsecure channels) we have to create a toy machine (the reason is because the needed algebra for the creation of those inventions could complicate the demonstration of the difference between P and NP).

Firstly we say that there is a correspondence between three known datas: X, Y and Z. But demonstrating the correspondence is there, we will have to construct before the parameters which factorize it: A, B, C and D.

For that, we will imagine the world is like a Hilbert Space (everything bounded): in our universe everything is a plane and it is quantified. For that reason the only one way of correspondence which could be acceptable is with the latin squares, and no other better way. From this point, we can associate X with Y saying X is the row of the latin square and Y is the value gotten in the table after choicing the row X with any value to the column. So, if we want to create a correspondence between X and Y we will need a parameter (the column), and this one will be D.

Now we have to opperate: we take the D parameter for combining (as a row) with the Y (as a column) in other latin square, it will return us the X value. The value that will make it possible will be the C parameter. At this point, we can say the number of latin squares is trapped in the C parameter, because the square which allow us to relationate a row with the value needed to get the column is not only a latin square, in fact there are some. That is trivial of understanding.

Getting two values (C and D) we can get the values A and B. If we want to see that more clearly, we will understand the values of X and C like representing permutations of even values (X_0 and C_0). From this point we calculate:

$$A = X_0 – C_0$$

Later, we will get the values Y, D and X again, and we will understand them like permutations of odd values (Y_1, D_1 and X_1) to calculate:

$$B = Y_1 – D_1 – X_1$$

At this point we will undertand that knowing whether X, X_0 or X_1 we will be able of knowing the other two. However our system needs another dimension: the value of Z like the result of applying the original latin square the A as row and D as column.

With this soup of letters, and considering the necesity of constructing the mininum number of correspondences, we now are just prepared to initiate our travel to the study of the “hidding” correspondences.

As result, known the values X, Y, and Z, what are the parameters we could get to know in a bounded time? With a Hilbert universe the bound is important very much, because if it is not bounded all the reasons will be changed. But the fact is that if we only know the values X, Y and Z we won’t absolutelly deduct any parameter. However, we will always can find solutions from the knowledge of A, to know easily C and only C. Moreover, if we use as method the knowledge of B, then we will only know easily D and only D. The why of this result is because there is a multidependence between D and C, broken in an unknown sense when we know the value of Z (which it comes from the connection between A and D) with independence of the rest of calculations.

So getting an information without contradictions from the begining (X, Y, Z) and a choiced method (specifically method B) we will be not allowed to get the value of C, when the value exists.

After getting the knowledge of the bounded values A, B, C, D, it will always validate the coordinates (X, Y, Z) to get an easily way of validating, for that we can also clasify this problem in NP.

In conclussion, known the values X, Y, Z related with a fix latin square and two unknown parameters, we must quest whether the known value B generates or not, a possible A which will validate every said relation. The procedure to find it will need the study of every formation of a latin square. That number is always up to the length of the set of all values codifiable in the entry.

For that reason, there cannot be a polynomial bound in the formation of the deduction.