

# Mathematical Theory of the Square Puzzle

Luca Ghezzi

March 8, 2009

## 1 Introduction

This short account describes a possible algebraic approach to solve the square puzzle (see <http://www.geniopensante.it/doc/album/album.html>). The spirit of the puzzle is simply to have fun by playing a logic game and the spirit of this writing is simply to point out how easy the puzzle is, despite it could seem not at a first glance. We will only need the elementary concepts of matrix, remainder class and modular arithmetic.

The main result consists in showing that all possible configuration may be reached from the initial one according to the rules of the game. As a consequence, not only it is possible to find a path from the initial to the final configuration (i.e., the game may be solved from the scratch), but it also possible to find a path from any configuration to the final one, via the initial one (i.e., the game may be solved starting from any random configuration). The solvability proof is constructive, and an algorithm is produced to directly find a path connecting any two configurations. The algorithm is implemented by Javascript in an automatic solver that can be found by following the aforementioned link.

## 2 Algebraic premise

Some very basic algebraic tools are hereafter recalled, for the reader's convenience.

### 2.1 The field $\mathbb{Z}_2$

Let  $\mathbb{Z} := \{0, \pm 1, \pm 2, \dots\}$  be the ring of integers and  $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\} = \{2n | n \in \mathbb{Z}\}$ . Then the quotient  $\mathbb{Z}_2 := \mathbb{Z}/2\mathbb{Z}$  consists of the cosets  $0 + 2\mathbb{Z}$  and  $1 + 2\mathbb{Z}$  and is thus in bijective correspondence with (and virtually equivalent to)  $\{0, 1\}$ , the set of equivalence classes of remainders that result from dividing integers by 2. Then 0 (actually the equivalence class  $[0]_2$ , to be precise) stands for (the class of) even numbers, whilst 1 (actually the equivalence class  $[1]_2$ ) stands for (the class of) odd numbers. In the sequel, brackets will always be dropped when dealing with remainder classes, for the sake of brevity. It is easily shown that  $(\mathbb{Z}_2; +, \cdot)$ , i.e.,  $\mathbb{Z}_2$  endowed with the usual sum and product modulo

2, is a field (more generally, the ring of the remainder classes modulo  $p$ , denoted by  $(\mathbb{Z}_p; +, *)$  is a field iff  $p$  is prime).

## 2.2 The vector space $\mathcal{M}$

Let us now introduce the set  $\mathcal{M}$  of  $4 \times 4$  square matrices with entries in  $\mathbb{Z}_2$ . In the following, let us denote such matrices with bold uppercase letter (e.g.,  $\mathbf{A}$ ,  $\mathbf{B}$ ) and their general  $i, j$ -th entry by the relevant lower case letter (e.g.,  $a_{ij}$ ,  $b_{ij}$ , respect.). Let  $\mathbf{O}$  and  $\mathbf{Y}$  be, respect., the matrix with all coefficients equal to 0 (i.e., the null matrix) and equal to 1. Moreover, let  $\mathbf{U}_{ij} \in \mathcal{M}$  be the matrix such that  $u_{ij} = 1$ , whilst all the other entries are null. Let  $+$  :  $\mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M}$  be the usual (componentwise) sum of matrices. The set  $(\mathcal{M}; +)$  is trivially seen to be an abelian group.

Let  $\cdot$  :  $\mathbb{Z}_2 \times \mathcal{M} \rightarrow \mathcal{M}$  be the usual external product defined such that  $(c \cdot \mathbf{A})_{ij} = c \cdot a_{ij} \ \forall i, j \in \{1, \dots, 4\}$  (the product symbol is frequently dropped, for the sake of notational compactness). Then  $\mathcal{M}$  is a vector space over the field  $\mathbb{Z}_2$ . Such vector space is spanned by the set of the 16 matrices  $\mathbf{U}_{ij}$ , that is,  $\mathcal{M} = \text{span}\{\mathbf{U}_{ij} \mid i, j \in \{1, \dots, 4\}\}$ . Hence, we can express the general matrix  $\mathbf{A} \in \mathcal{M}$  as

$$\mathbf{A} = \sum_{i,j=1}^4 a_{ij} \cdot \mathbf{U}_{ij}. \quad (1)$$

In the latter we will refer to (1) as the *canonical decomposition* of  $\mathcal{M}$ .

## 3 Matrix transformations

### 3.1 Basis transformations

We define, for  $i, j \in \{1, \dots, 4\}$  and for some  $k$ , a set of applications, termed *basis transformations*,

$$f_{k,ij} : \mathcal{M} \rightarrow \mathcal{M}$$

as follows. Let  $f_{1,ij}$  be an application that adds 1 modulo 2 to the  $i, j$ -th coefficient of a given matrix  $\mathbf{A}$  and so does also for the coefficients in position  $i, j - 1$ ;  $i, j + 1$ ;  $i - 1, j$  and  $i + 1, j$ . In other words,  $f_{1,ij}$  changes the value from 1 to 0 or from 0 to 1 of the coefficients forming a cross centered on the  $i, j$ -th element. In case the center of the cross is close the “border” of the matrix (i.e.,  $i = 1$  or  $i = 4$  or  $j = 1$  or  $j = 4$ ), then it is intended that the shape of the cross has to be applied as the matrix was a torus (i.e., if  $i = 1$ , then  $i - 1 = 4$ ; if  $i = 4$ , then  $i + 1 = 1$ ; and likewise for  $j$ ). As an example, here we show a sample matrix  $\mathbf{A}$  and its basis transformed  $f_{1,21}(\mathbf{A})$ :

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad f_{1,21}(\mathbf{A}) = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Analogously, we may define many other basis transformations by using other shapes instead of a cross. The shape of other transformations that we take into account are shown in fig. 1, together with their identifier  $k$ . The number of the coefficients having their values swapped by the basis transformations in fig. 1 is always odd. This is a precise choice whose necessity will be clear from what follows.

### 3.2 Global transformations

Basis transformations are used to define the relevant *global transformations*. Particularly, we define the global transformation

$$F_k : \mathcal{M} \rightarrow \mathcal{M}$$

as

$$F_k(\mathbf{U}_{ij}) = f_k(\mathbf{U}_{ij}), \quad \forall i, j \in \{1, \dots, 4\}, \quad (2)$$

for the canonical base of  $\mathcal{M}$  and, with reference to the canonical base decompositions (1), as

$$F_k(\mathbf{A}) = F_k \left( \sum_{i,j=1}^4 a_{ij} \cdot \mathbf{U}_{ij} \right) = \sum_{i,j=1}^4 a_{ij} \cdot F_k(\mathbf{U}_{ij}) \quad (3)$$

for a generical matrix  $\mathbf{A} \in \mathcal{M}$ .

One may easily verify that any global transformation is obtained by applying the relevant basis transformation  $f_{k,ij}$  to all the coefficients equal to 1 in the input matrix. With the previous expression, we mean, as obvious, that the “original” coefficients equal to 1 have to be recorded and then  $f_{k,ij}$  has to be applied to them and to them only, without considering coefficients previously

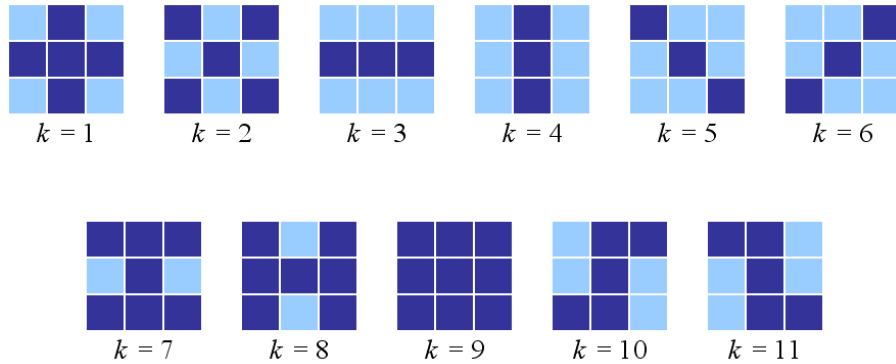


Figure 1: The “shapes” of basis transformations.

null and then swapped to 1 by the first and subsequent applications of the basis transformation, and without forgetting coefficients originally equal to 1 and then swapped to 0. As an example, here we show a sample matrix  $\mathbf{A}$  and its global transformed  $F_1(\mathbf{A})$ , where  $F_1$  is the global transformation associated with the cross shaped basis transformation:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad F_1(\mathbf{A}) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

## 4 Properties of global transformations

Global transformations have some nice properties that will allow to solve the puzzle.

### 4.1 Global transformations on special matrices

First, it is obvious that

$$F_k(\mathbf{O}) = \mathbf{O}, \quad \forall k, \quad (4)$$

since there is no coefficient equal to 1 in  $\mathbf{O}$ . Then

$$F_k(\mathbf{Y}) = \mathbf{O}, \quad \forall k, \quad (5)$$

for, since each basis transformation affects an odd number of cells, then each entry of  $\mathbf{Y}$  falls into the shape of an odd number of other entry centered basis transformations, so that the value of any entry is changed an odd number of times, that means, any entry passes from 1 to 0.

### 4.2 Linearity

One may also notice that

$$F_k(c \cdot \mathbf{A}) = c \cdot F_k(\mathbf{A}), \quad \forall c \in \mathbb{Z}_2, \forall \mathbf{A} \in \mathcal{M}, \forall k, \quad (6)$$

for, if  $c = 0$  then  $F_k(0 \cdot \mathbf{A}) = F_k(\mathbf{O}) = \mathbf{O} = 0 \cdot F_k(\mathbf{A})$  for property (4), whilst if  $c = 1$  then trivially  $F_k(1 \cdot \mathbf{A}) = F_k(\mathbf{A}) = 1 \cdot F_k(\mathbf{A})$ .

Moreover,

$$F_k(\mathbf{A} + \mathbf{B}) = F_k(\mathbf{A}) + F_k(\mathbf{B}), \quad \forall \mathbf{A}, \mathbf{B} \in \mathcal{M}, \forall k. \quad (7)$$

The proof is straightforward by recalling defining property (3) and the canonical decomposition (1):

$$F_k(\mathbf{A} + \mathbf{B}) = F_k \left[ \sum_{i,j=1}^4 (a_{ij} + b_{ij}) \mathbf{U}_{ij} \right] = \sum_{i,j=1}^4 (a_{ij} + b_{ij}) F_k(\mathbf{U}_{ij}) = F_k(\mathbf{A}) + F_k(\mathbf{B}).$$

Joining property (6) and (7), one finds that global transformations are vector space homomorphisms, that means, linear applications from  $\mathcal{M}$  onto itself, or

$$F_k(c \cdot \mathbf{A} + d \cdot \mathbf{B}) = c \cdot F_k(\mathbf{A}) + d \cdot F_k(\mathbf{B}), \quad \forall c, d \in \mathbb{Z}_2, \forall \mathbf{A}, \mathbf{B} \in \mathcal{M}, \forall k. \quad (8)$$

It is well known that the powers of linear functionals are linear as well, so that

$$F_k^n(c \cdot \mathbf{A} + d \cdot \mathbf{B}) = c \cdot F_k^n(\mathbf{A}) + d \cdot F_k^n(\mathbf{B}), \quad \forall c, d \in \mathbb{Z}_2, \forall \mathbf{A}, \mathbf{B} \in \mathcal{M}, \forall k. \quad (9)$$

The proof is straightforwardly produced by induction:

$$\begin{aligned} F_k^n(c\mathbf{A} + d\mathbf{B}) &= F_k F_k^{n-1}(c\mathbf{A} + d\mathbf{B}) = F_k(cF_k^{n-1}(\mathbf{A}) + dF_k^{n-1}(\mathbf{B})) \\ &= cF_k F_k^{n-1}(\mathbf{A}) + dF_k F_k^{n-1}(\mathbf{B}) = cF_k^n(\mathbf{A}) + dF_k^n(\mathbf{B}). \end{aligned}$$

### 4.3 Nilpotence

Property (9) obviously holds in the special case when  $n = 2$ , that is, for squares of global transformations. Actually, for all higher powers the reasoning becomes trivial, since global transformations are nilpotent. To see this, one may first notice that

$$F_k^2(\mathbf{U}_{ij}) = \mathbf{O}, \quad \forall i, j \in \{1, \dots, 4\}. \quad (10)$$

The proof is actually a trivial check. Thanks to the ‘‘thoroidal’’ nature of the transformations, it is sufficient to check for a single couple  $i, j$  of indices. As an example, we hereby report the case of  $F_1$ :

$$\mathbf{U}_{22} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad F_1(\mathbf{U}_{22}) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad F_1^2(\mathbf{U}_{22}) = \mathbf{O}.$$

It can be easily verified by exhaustive testing that the same holds also for all of the other transformations previously defined. For those eager to know the hidden reasons of things, the parity of the number of value swaps must be considered. When we apply twice any global transformation to a canonical base matrix, the only coefficient valued 1 is swapped an odd number of times (and then it is set to 0), whereas all the other coefficients are swapped an even number of times, so that they remain null. Obviously, this is due to the fact that any basis transformation is such to affect an odd number of coefficients. It can be readily understood that global transformation nilpotence is not only due to the shape of basis transformation, but also to the size 4 of matrices belonging to  $\mathcal{M}$ .

From this point on, the finalization of the argument is a real triviality. Nilpotence in the general case, that is,

$$F_k^2(\mathbf{A}) = \mathbf{O}, \quad \forall \mathbf{A} \in \mathcal{M}, \forall k, \quad (11)$$

follows straightforwardly by combining the linearity of squares of global transformations (9) with canonical decomposition (1) and nilpotence of canonical base matrices (10), that is,

$$F_k^2(\mathbf{A}) = F_k^2 \left( \sum_{i,j=1}^4 a_{ij} \mathbf{U}_{ij} \right) = \sum_{i,j=1}^4 a_{ij} F_k^2(\mathbf{U}_{ij}) = \sum_{i,j=1}^4 a_{ij} \mathbf{O} = \mathbf{O}.$$

## 5 Formalization and solution of the game

We now apply the previous formalism and results to set the mind puzzle of the square in the framework of our theory and then to solve it. An implementation of the puzzle may be found on-line at <http://www.geniopensante.it/doc/album/album.html>, where the reader is referenced.

### 5.1 Description of the puzzle

The aim of the game is to produce a fully colored picture by clicking onto the cells composing a  $4 \times 4$  array. Each click will switch the color, from grayscale to colored or viceversa, of those cells belonging to a neighborhood with prescribed shape, as shown fig. 1. The array is supposed to have a toroidal topology, so that the top side is identified with the bottom one and the right side is identified with the left one, according to the standard 2D model of a torus.

First, it should be obvious that the matrices in  $\mathcal{M}$  are in one-to-one correspondence with the possible configurations of the game, and that basis transformations correspond to the action of clicking onto a cell. Since there are 16 cells, each of which may have 2 states, there are  $2^{16} = 65536$  total possible states, one of which is the final goal. Therefore, global transformations are simply the action of clicking onto a set of cells, as already described previously.

### 5.2 Solution of the puzzle from the scratch

The game initial all-gray configuration is associated with matrix  $\mathbf{Y}$  and the sought final all-colored configuration is associated with the null matrix  $\mathbf{O}$ . Hence, from (5), to solve the game starting with the initial all-gray configuration one must click onto each cell exactly once (no matter the order, obviously!).

### 5.3 Solution of the puzzle from a random configuration

Due to nilpotence property (11), to solve the game starting from any other configuration (associated to a matrix  $\mathbf{A} \in \mathcal{M}$ ), all one needs is to transform twice that configuration. That is precisely what is done by an autosolver implemented in the web page as Javascript code.

## 5.4 Path connectedness of $\mathcal{M}$ under transformations

It can also be noticed that there is a path in  $\mathcal{M}$  produced by successive (global, and thus also basis) transformations and connecting any two configurations (associated to matrices  $\mathbf{A}, \mathbf{B} \in \mathcal{M}$ ), for, if one can solve any configuration, then there is a path connecting matrix  $\mathbf{A}$  (and similarly  $\mathbf{B}$ ) to the null matrix  $\mathbf{O}$ . Then, since applying the same transformation (i.e., clicking onto the the very same cells) will revert the path and allow passing from the null matrix  $\mathbf{O}$  to  $\mathbf{A}$  (or similarly to  $\mathbf{B}$ ), then to connect  $\mathbf{A}$  to  $\mathbf{B}$  is always possible by passing from  $\mathbf{A}$  to  $\mathbf{O}$  and then from  $\mathbf{O}$  to  $\mathbf{B}$ . The reverse path is obtained likewise.

Finally, one may also notice that clicking onto all the cells of a basis transformation shape will change only the value of the “central” cell. The reason is once again due to the parity of the number of swaps. This immediately suggests a way to construct a path from any matrix to another one differing only by a single entry. Connecting path may therefore be drawn by working componentwise. This way, many basis transformations will be carried out many times, but the parity of the number of repetitions may be remembered and only those basis transformations applied an odd number of times may be actually applied, and just once.