Problem 7 : An experiment

Team : France 2

ITYM 2012

Abstract

In this problem, we begin in question 1.a. by giving the number of balanced n-tuples X for which $\alpha(X)$ is balanced. Using combinatorics methods on batches of "0" and "1", we first show that we must have $n = 4p$ and then find that the number of such n-tuples is $2\binom{2p}{p}\binom{2p-1}{p-1}$.

We solved the case $\alpha^2(X)$ is also balanced using the same type of reasoning. The expression we find is much more complicated. We then find by induction a formula for α^n, which we can get using matrices.

We give a few ideas about super-balanced n-tuples, question 1.b.. For example our formula yields that there is no super-balanced n-tuple if n is a power of 2.

We then generalize our methods of question 1.a to n-tuples containing an arbitrary number of "1".

We conclude by giving a few ideas about another generalization, considering other endomorphisms than α. For several nontrivial endomorphisms we found the number of balanced n-uples which have a balanced image.

Question 1.a.

Let n be a positive integer. X is a n-tuple, $X \in (\mathbb{F}_2)^n$:

$$X = (x_1, ..., x_n)$$

We define the operation α :

$$\alpha(X) = (x_1 + x_2, ..., x_n + x_1)$$

Number of balanced n-tuples X for $n = 2q$

It is clear that if X is balanced, then we have n is even : $\exists q \in \mathbb{N}, n = 2q$. Indeed we have q "0" and q "1" in the n-tuple.
We can build a balanced n-tuple :
- we number the n elements of the n-tuple ;
- we choose the place of the q "0", we have $\binom{n}{q} = \binom{2q}{q}$ choices ;
- we place the q "1" in the q empty places left.

Hence we have $\binom{2q}{q}$ balanced $2q$-tuples for every $q \in \mathbb{N}$.

We will show that if X and $\alpha(X)$ are balanced, then $\exists p \in \mathbb{N}, n = 4p$.

We notice that a "1" appear in $\alpha(X)$, if and only if we have "0,1" or "1,0" in X, because 1+1 = 0 and 0+0 = 0 and 1+0 = 1.
We consider X as a sequence of batches of "1" and batches of "0", so we have a "1" in $\alpha(X)$, when we change of batch.
Without loss of generality, let's assume that in X, $x_1 = 1$ and $x_n = 0$, making if necessary a cyclic permutation. We know that X is balanced, so we have a "1" and a "0".
Then we have as many batches of "1" as batches of "0". We have an even number of batches, so we change of batch an even number of times. (We count the last change of batch when we have $x_1 + x_n$.) Then we have an even number of "1" in $\alpha(X)$.
We have shown that $n = 2q$, so n is congruent to 2 or 0 modulo 4.
If $n \equiv 0[4]$ and $n = 2q$, then q is even.
If $n \equiv 2[4]$ and $n = 2q$, then q is odd.
In $\alpha(X)$, we have an even number of "1", so it can be balanced for $n \equiv 0[4]$, because we can have q "1" in $\alpha(X)$, but for $n \equiv 2[4]$, it can't be balanced, because q is odd. To conclude, if X and $\alpha(X)$ is balanced, then $\exists p \in \mathbb{N}, n = 4p$.

Number of balanced n-tuples X such that $\alpha(X)$ is balanced

Lemma : There are $\binom{n+k-1}{n-1}$ n-tuples of $\mathbb{N}^n$ of sum k ($k \in \mathbb{N}$).

We can build a balanced n-tuple X such that $\alpha(X)$ is balanced. We must have $n = 4p$. We want to have $2p$ "1" in $\alpha(X)$. Hence we must have exactly $2p$ changes of batch, i.e. $2p$ batches, i.e. p batches of "1" and p batches of "0", since we have as many batches of "1" as batches of "0".

Without loss of generality, we suppose that X starts with a "1" ($x_1 = 1$). Let's build our n-tuple :

$$X = (\underbrace{1, .., 0, ...,} ..., \underbrace{1, ..., 0, ...,} ...)$$

- we place a one "1" in each batch of "1" and a "0" in each batch of "0" ;
- we have p "1" left, which have to be placed in p batches of "1", one of which is splited in two batches, so we have to place p "1" in $p+1$ batches. The number of choices is the number of $p+1$-tuples of $\mathbb{N}^{p+1}$, sum of which is p, i.e $\binom{2p}{p}$.
- we have p "0" left, which have to be placed in p batches of "0". The number of choices is the number of p-tuples of $\mathbb{N}^p$, sum of which is p, i.e $\binom{2p-1}{p-1}$.

When X starts with a "1", we have $\binom{2p}{p}\binom{2p-1}{p-1}$ choices. The number of balanced n-tuples X such that $\alpha(X)$ is balanced is $2\binom{2p}{p}\binom{2p-1}{p-1}$ for each $n = 4p$.

<u>Proof of the lemma</u> : Let's consider the number of elements of $\mathbb{N}^{*n}$ of sum $k \in \mathbb{N}*$. One element corresponds to a unique repartition of $n-1$ sticks between k balls :

There is $k-1$ places between the balls and we must place $n-1$ sticks, we have $\binom{k-1}{n-1}$ choices. The number of elements of $\mathbb{N}^{*n}$ of sum $k \in \mathbb{N}*$ is $\binom{k-1}{n-1}$.

To find the number of elements of $\mathbb{N}^n$ of sum $k \in \mathbb{N}$, we associate at each number x of the element, the number $x+1$. Then we have an element of $\mathbb{N}*^n$ of sum $n+k$. Hence the number of elements of $\mathbb{N}^n$ of sum $k \in \mathbb{N}$ is $\binom{n+k-1}{n-1}$.

Number of balanced n-tuples X such that $\alpha(X)$ and $\alpha^2(X)$ are balanced

We've just built a balanced n-tuples X such that $\alpha(X)$ is balanced. In $\alpha(X)$, we have $2p$ "1". To have $\alpha^2(X)$ balanced, we must have p batches of "1". Then, we notice that each "0" corresponds to "1,1" or "0,0" and separates two batches of "1". Then to have p batches of "1" in $\alpha(X)$, we must have p batches of "1" or "0" with only one element, then this leads to no "0".

$$X = (\underbrace{1, .., 0, ...,} ..., \underbrace{1, ..., 0, ...,} ...)$$

Let's build such a X, supposing it starts with a "1", without loss of generality :
- we place a one "1" in each batch of "1" and a "0" in each batch of "0" ;
- we choose the number k of batches of "0" with a unique element We must have at least one batch with more than one element. Then $k \in \{0, ..., p-1\}$;
- we choose among the p batches of "0", the k batches, in which we put no more "0" : $\binom{p}{k}$;
- we place the p "0" left in the $p-k$ batches left : the number of $p-k$-tuples of $\mathbb{N}^{*p-k}$, sum of which is p : $\binom{p-1}{p-k-1}$;
- we choose among the p batches of "1", the $p-k$ batches with a unique element, remenbering that there is the first batch of "1", which is splited in two batches : one at the beginning, one

at the end, which can be empty : we have $p+1$ batches to complete. Then : $\binom{p}{p-k}$, indeed $\binom{p-1}{p-k-1}$ when we take the splited batch and $\binom{p-1}{p-k}$ when we don't take it;
- we place the p "1" left in the $p-(p-k)=k$ batches :

- If we have the splited batch to complete, we have to place p "1" in $k+1$ batches : the number of $k+1$-tuples of $\mathbb{N}^{*k+1}$, sum of which is p : $\binom{p-1}{k}$;
- If we haven't the splited batch to complete, we have to place p "1" in k batches :the number of k-tuples of $\mathbb{N}^{*k}$, sum of which is p : $\binom{p-1}{k-1}$.

To conclude, we count the number N of X starting with a "1" and such that $\alpha(X)$ and $\alpha^2(X)$ is balanced :

$$N=\sum_{k=0}^{p-1}\binom{p}{k}\binom{p-1}{p-k-1}\left(\binom{p-1}{p-k-1}\binom{p-1}{k-1}+\binom{p-1}{p-k}\binom{p-1}{k}\right)$$

We have $2N$ balanced n-tuples X such that $\alpha(X)$ and $\alpha^2(X)$ are balanced.

An expression of $\alpha^k(X)$, $k\in\mathbb{N}$

Let P_k :

$$\alpha^k(X)=(\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+0)[n]},...,\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+j)[n]},...),j\in\{0,...,n-1\}$$

We will show P_k for every $k\in\mathbb{N}$ by induction.
- Basis for $k=0$:

$$\alpha^0(X)=(x_1,..,x_j,...)=(\sum_{i=1}^{0+1}\binom{0}{i-1}x_{(i+0)[n]},...,\sum_{i=1}^{0+1}\binom{0}{i-1}x_{(i+j)[n]},...)$$

$j\in\{0,...,n-1\}$
P_0 is true.
- Inductive step :
We suppose that P_k is true for some $k\in\mathbb{N}$:

$$\alpha^k(X)=(\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+0)[n]},...,\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+j)[n]},...),j\in\{0,...,n-1\}$$

Then

$$\begin{aligned}\alpha^{k+1}(X)=(&\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+0)[n]}+\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+1)[n]},...,\\&\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+j)[n]}+\sum_{i=1}^{k+1}\binom{k}{i-1}x_{(i+j+1)[n]})\end{aligned}$$

$$\alpha^{k+1}(X) = (\sum_{i=2}^{k+1}\left[\binom{k}{i-1}+\binom{k}{i}\right]x_{(i+0)[n]} + \binom{k}{0}x_1 + \binom{p}{p}x_{(k+2)[n]}, ...,$$
$$\sum_{i=2}^{k+1}\left[\binom{k}{i-1}+\binom{k}{i}\right]x_{(i+j)[n]} + \binom{k}{0}x_{j+1} + \binom{p}{p}x_{(j+k+2)[n]}, ...)$$

$$\alpha^{k+1}(X) = (\sum_{i=1}^{k+2}\binom{k+1}{i-1}x_{(i+0)[n]}, ..., \sum_{i=1}^{k+2}\binom{k+1}{i-1}x_{(i+j)[n]}, ...)$$

P_{k+1} is true.

- Conclusion : P_k is true for all $k \in \mathbb{N}$.

A matrix

To find the previous expression, we can consider the matrix $n \times n$ A :

$$A = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 \\ 1 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 1 & 0 \\ 0 & \cdots & 0 & 1 & 1 \end{pmatrix}$$

To apply A to $X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix}$ is equivalent to apply α : $XA = \alpha(X)$. Then to apply α^k is to apply A^k.
We notice that A is the sum of the identity matrix I and a circulant matrix C :

$$A = I + C = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

With the matrix I, we have : $IC = CI = C$, then we can use the Newton's binom :

$$A^k = (I + C)^k = \sum_{i=0}^{k}\binom{k}{i}I^{k-i}C^i = \sum_{i=0}^{k}\binom{k}{i}C^i$$

With this expression, we find the previous expression again.

Question 1.b

Power of 2

If n is a power of 2,then 2 divides $\binom{n}{i}$, when $i \in \{1, ..., n-1\}$. Then we have, using the previous expression and putting away all the even terms :

$$\alpha^n(X) = (x_1 + x_{(1+n)[n]}, ..., x_j + x_{(j+n)[n]}, ...) = (2x_1, ..., 2x_j, ...) = (0, ..., 0, ...)$$

There is no super-balanced n-tuples, when n is a power of 2.

Super-balanced n-tuples

If X and $\alpha(X)$ are balanced, then $\exists p \in \mathbb{N}, n = 4p$.
Then, if we want to find any superbalanced n-tuples, we must search with $n = 4p$ when p isn't a power of 2.

A cycle

We notice that we have a finite number of n-tuples X, indeed 2^n. Hence, if we've applied 2^n times α, we have $2^n + 1$ n-tuples. Thanks to the Pigeonhole principle, we know that at least one n-tuple appears at least twice. Therefore, when we have the same n-tuples, we have the same following n-tuples : we have a cycle. Hence, to find a super-balanced n-tuple, we have a finite number of cases to see. If (0,0,...,0) appears, we have always (0,0,...,0) after.

Question 2

A new property

We can count the number of n-tuples X containing k "1" with $0 \leq k \leq n$, it remains to count the number of choices when we have to place k "1" among n places : $\binom{n}{k}$.

Folowing the same idea, we can count the number of X containing k "1", such that $\alpha(X)$ contains k "1". To have k "1", we must have k changes of batch. We notice that k must be even : $\exists d \in \mathbb{N}^*, k = 2d$. To have k "1", we must have k changes of batch, so k batches, so d batches of "1" and d batches of "0". Without loss of generality, we suppose that X starts with a "1" ($x_1 = 1$). Let's build our n-tuple :

$$X = (\underbrace{1, .., 0, ...,}, ..., \underbrace{1, ..., 0, ...,} ...)$$

- we place a one "1" in each batch of "1" and a "0" in each batch of "0" ;
- we have d "1" left, which have to be placed in d batches of "1", one of which is splited in two batches, so we have to place d "1" in $d+1$ batches. The number of choices is the number of $d+1$-tuples of $\mathbb{N}^{d+1}$, sum of which is d, i.e $\binom{2d}{d}$.

- we have $n-k-d=n-3d$ "0" left, which have to be placed in d batches of "0". The number of choices is the number of d-tuples of $\mathbb{N}^d$, sum of which is $n-3d$, i.e $\binom{n-2d-1}{d-1}$.
When X starts with a "1", we have $\binom{2d}{d}\binom{n-2d-1}{d-1}$ choices. The number of n-tuples X containing k "1" such that $\alpha(X)$ contains k "1" is $2\binom{2d}{d}\binom{n-2d-1}{d-1}$ for each $k=2d$, we notice that k is necessary inferior to $n-1$.

We've just built a n-tuples X containing k "1" such that $\alpha(X)$ contains k "1". To have $\alpha^2(X)$ with k "1", we must have d batches of "1". Each "0" corresponds to "1,1" or "0,0" and separates two batches of "1". Then to have d batches of "1" in $\alpha(X)$, we must have d batches of "1" or "0" with only one element, then this leads to no "0".
Let's build such a X, supposing it starts with a "1", without loss of generality :
- we place a one "1" in each batch of "1" and a "0" in each batch of "0" ;
- we choose the number l of batches of "0" with a unique element. We must have at least one batch with more than one element, when $k \neq 0$. Then $l \in \{0, ..., d-1\}$;
- we choose among the d batches of "0", the l batches, in which we put no more "0" : $\binom{d}{l}$;
- we place the $n-3d$ "0" left in the $d-l$ batches left : the number of $d-l$-tuples of $\mathbb{N}^{*d-l}$, sum of which is $n-3d$: $\binom{n-3d-1}{d-l-1}$;
- we choose among the d batches of "1", the $d-l$ batches with a unique element, remenbering that there is the first batch of "1", which is splited in two batches : one at the beginning, one at the end, which can be empty : we have $d+1$ batches to complete. Then : $\binom{d}{d-l}$, indeed $\binom{d-1}{d-l-1}$ when we take the splited batch and $\binom{d-1}{d-l}$ when we don't take it;
- we place the d "1" left in the $d-(d-l)=l$ batches :

- If we have the splited batch to complete, we have to place d "1" in $l+1$ batches : the number of $l+1$-tuples of $\mathbb{N}^{*l+1}$, sum of which is d : $\binom{d-1}{l}$;
- If we haven't the splited batch to complete, we have to place d "1" in l batches : the number of l-tuples of $\mathbb{N}^{*l}$, sum of which is d : $\binom{d-1}{l-1}$.

To conclude, we count the number N of X starting with a "1" and such that $\alpha(X)$ and $\alpha^2(X)$ is balanced :

$$N = \sum_{l=0}^{d-1} \binom{d}{l}\binom{n-3d-1}{d-l-1}\left(\binom{d-1}{d-l-1}\binom{d-1}{l-1} + \binom{d-1}{d-l}\binom{d-1}{l}\right)$$

We have $2N$ n-tuples X containing $k=2d$ "1" such that $\alpha(X)$ and $\alpha^2(X)$ contain k "1".

Generalization problem

Let $(B_i)_{i\in\mathbb{N}}$ be a family of matrices $n \times n$, with $\forall (i,j) \in \{1, ...n\}, x_{i,j} \in \mathbb{F}_2$:

$$B_i = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n} \end{pmatrix}$$

We can consider a function β_i, which corresponds to the matrix B_i in this family such that $\beta_i(X) = XB_i$ and then count the number of balanced X such that $\beta_i(X)$ is balanced too, and so on.

Some functions, which keep the balanced property of X

- For all even integer n, the permutations P keep the balanced property of X :

  $$P(X) = (f(x_1), ..., f(x_n))$$

  The function f is a bijection from $\{x_1, ..., x_n\}$ to $\{x_1, ..., x_n\}$.
  There is $n!$ permutations.
  The matrix associated to a permutation is such that there is a "1" for each column and for each line.
  For example :

  $$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

  Then $P(X) = (x_3, x_1, x_5, x_2, x_6, x_4)$

- Let's consider the functions, which correspond to the matrices, which are such that there is a "0" for each column and for each line. Then each terms in the image is the sum of all the terms of X minus one of them, always a different one. Since we are in $\mathbb{F}_2$ and that X is balanced :

  $$S = \sum_{j=1}^{n} x_j = \frac{n}{2} \times 1 + \frac{n}{2} \times 0$$

  If $n \equiv 0[2]$, we have $S = 0$. And then, we have $\frac{n}{2}$ times $S - 1 = 1$ and $\frac{n}{2}$ times $S - 0 = 0$.
  If $n \equiv 2[2]$, we have $S = 1$. And then, we have $\frac{n}{2}$ times $S - 1 = 0$ and $\frac{n}{2}$ times $S - 0 = 1$.
  If X is balanced, the image is balanced. These matrices keep the balanced property.
  There is $n!$ matrices like that.
  For example :

  $$T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

  Then $T(X) = (S - x_3, S - x_1, S - x_5, S - x_2, S - x_6, S - x_4)$

Some functions, which keep the balanced property of some X

We want to find some functions, which keep the balanced property of some X, and the number of X touched.

- Let's consider the functions, which correspond to the matrices, which are such that there is a "1" per column and per line, except for one line and one column.
For example :
$$Q = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$
Then $Q(X) = (x_3, x_1, x_5, x_2 + x_4, x_6, x_4)$
Then we have a permutation and the addition of one element for a place. If X is balanced, we have as many "1" as "0". In the image, every term appears once except one, because another one is added to it. If the term which is added is "0", it doesn't change the term, to which it is added. Then it keeps the balanced property. But, if it is a "1", it changes the term. Then it doesn't keep the balanced property. Then every balanced X, which have a "0" at this place, is such that their image is balanced, we have to place the $q-1$ "0" left among the $2q-1$ places : $\binom{2q-1}{q-1}$ for $n = 2q$

- Let's consider the functions, which correspond to the matrices, which are such that there is a "1" per column and per line, and at which we've added two "1".
For example :
$$R = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$
Then $R(X) = (x_3, x_1 + x_5, x_5, x_2 + x_4, x_6, x_4)$
We can see that there one or two disturbations : eather we have a sum of three terms, or we have two sums of two terms.
In the first case, the sum of the two terms added must equal "0", it must be two "1" or two "0". If it is two "1", we have to place $q-2$ "1" left in $2q-2$ places. Same things with "0". Then we have $\binom{2q-2}{q-2}$ balanced X such that the image is balanced.
In the second case, there is several possibilities :

  - The terms, which are disturbed, equal "0". Then, the added terms must equal "0", in order not to add any "1". It concerns $\binom{2q-4}{q-4}$ X.
  - The terms, which are disturbed, equal "1" for one and "0" for the other. Not to change the number of "1", we must have two "1" or two "0". It concerns $4\binom{2q-4}{q-3}$. We have 4 choices for the 4 important terms. And then we place the "1" or the "0" left.
  - The terms, which are disturbed, equal "1". Then, the added terms must equal "0", in order not to add any "0". It concerns $\binom{2q-4}{q-4}$ X.

Then we have $2\binom{2q-4}{q-4} + 4\binom{2q-4}{q-3}$ balanced X such that the image is balanced.

Some functions, which behaves like α

- A is the sum of the identity matrix and a circulant matrix. We want to consider the other matrices like that and their effects to the balanced X. Let γ_i be a fonction associated to such a matrix $I + C_i$ with $1 \leq i \leq n-1$:

$$\gamma(X) = (x_1 + x_{(1+i)[n]}, ..., x_j + x_{(j+i)[n]}, ...)$$

  Like we've seen later, we have :

$$(I + C_i)^k = \sum_{l=0}^{k} \binom{k}{l} I^{k-l} C_i^l = \sum_{l=0}^{k} \binom{k}{l} C_i^l$$

- We notice that α corresponds to a matrix, which is the sum of the identity matrix and a circulant matrix, which is a particular form of a matrix, which corresponds to a permutation without fix point. So consider the matrices, which are the sum of identity matrix and a matrix, which corresponds to a permutation without fix point.
  For example :

$$B = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

  Then $\beta(X) = (x_1 + x_3, x_2 + x_1, x_3 + x_5, x_4 + x_2, x_5 + x_6, x_6 + x_4)$
  We want to know when these functions keep the balanced property of X.

- Let's consider the matrices, where there is two "1" per column and per line. On a line, we have the two "1" next to each other or one at the end and one at the beginning.

$$E = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

  Then $\beta(X) = (x_2 + x_5, x_5 + x_3, x_3 + x_4, x_4 + x_1, x_1 + x_6, x_6 + x_2)$ It remains to apply α to $X' = (x_2, x_5, x_3, x_4, x_1, x_6)$
  For each matrix like this, to apply the matrix is equivalent to apply A to a unique X', which is the image of X by a unique permutation. The matrix is the product of A and a matrix, which corresponds to a permutation. Then we can build the $2\binom{2p}{p}\binom{2p-1}{p-1}$ balanced X', which give us $2\binom{2p}{p}\binom{2p-1}{p-1}$ balanced X such that the image after the application of the matrix is balanced. When we apply the matrix twice, it becomes harder.