

Article

Grouping Problem II

TAKEUCHI, Kiyohiko*

Abstract

Consider to divide n^2 students into n groups with n members. One time dividing them, then reset the groups and divide them once more. Each new group satisfies the condition that the new group members belonged to the different groups each other in the first division. Repeat the division into groups consisting of members belonging to the different groups each other in the preceding divisions. How many times can you repeat the above divisions? This is equivalent to the classical famous problem asked Euler as the 36 Officers Problem in the end of the 18 century. The answer was given in several cases by many mathematicians. This paper shows that the easier answer of this problem is $n + 1$ if n is the power of prime.

Key words: orthogonal latin square, combinatorics, linear algebra, elementary number theory

1 Introduction

We consider the following question:

Question. Consider to divide n^2 students into n groups with n members. One time dividing them, then reset the groups and divide them once more. Each new group satisfies the condition that the new group members belonged to the different groups each other in the first division. Repeat the division into groups consisting of members belonging to the different groups each other in the preceding divisions. How many times can you repeat the above divisions?

This paper gives the answer of this question in the case $n = p^d$ the power of prime. The question above is equivalent to the one how many mutually orthogonal squares of order n . This has been treated by many mathematicians since 1782 when Euler began a study of a simple mathematical puzzle, the 36 Officers Problem which concerns a group of thirty-six officers of six different ranks, taken from six different regiments, and arranged in a square in a way such that in each row and column there are six officers, each of a different rank and regiment [Eul]. Our partial answer was already gotten by Bose [Bos] (or Moore [Moo]) using the finite projective geometry about one hundred years ago, but ours is given by more elementary linear-algebraic way. The simple case was treated in [Tak].

We use the following notation and definitions here.

Fix a positive integer $n \in \mathbb{Z}$. Let Z_n be the set of non-negative integers less than n :

$$Z_n = \{0, 1, 2, \dots, n-1\}.$$

For an integer $a \in \mathbb{Z}$, the symbol $[a]_n \in Z_n$ denotes the remainder of dividing a by n . For any set A , the symbol $|A|$ denotes the number of elements in A . Let $X = Z_n \times Z_n$ be a set of pairs (i, j) of non-negative integers i, j less than n . The set X has the canonical partition $\mathfrak{G} = \{G_i\}$ into n groups $G_i = \{(i, j) | j \in Z_n\}$ ($i \in Z_n$) with $|G_i| = n$. Our problem is considered how many times to get other partitions $\mathfrak{B}^{(k)} = \{B_j^{(k)}\}$ of X into n blocks with $|B_j^{(k)}| = n$ such that $|G_i \cap B_j^{(k)}| = |B_j^{(k)} \cap B_{j'}^{(k')}| = 1$ for any $i, j, j' \in Z_n$ and for any different k, k' .

Let \mathfrak{B} be a set of blocks in X satisfying the following three conditions :

(C1) $|B| = n$ for any block $B \in \mathfrak{B}$,

(C2) $|B \cap G_i| = 1$ for any block $B \in \mathfrak{B}$ and for any group $G_i \in \mathfrak{G}$, and

(C3) $|B \cap B'| \leq 1$ for any pair of different blocks $B, B' \in \mathfrak{B}$.

The previous problem is equivalent to estimating the maximal value of the number $|\mathfrak{B}|$. This paper gives the maximal value of $|\mathfrak{B}|$ in the case that n is the power of prime number $n = p^d$ for any $d \in \mathbb{N}$.

Main Result: The maximal value of $|\mathfrak{B}|$ is n^2 if $n = p^d$, the power of prime number. That is to say, in the case $n = p^d$, it can be repeated $n + 1$ times to divide n^2 students into n groups with n members, such that each pair of members belongs to the same group only one time.

This paper gives the block set \mathfrak{B} satisfying the above condition (C1), (C2), (C3) in the case $n = p^d$ ($d \in \mathbb{N}$). Section 2 shows that the upper bound of $|\mathfrak{B}|$ is n^2 . Section 3 constructs the block set \mathfrak{B} attaining the upper bound under the some assumption (A1), (A2). Section 4 asserts that (A1) and (A2) hold in the case $n = p^d$ ($d \in \mathbb{N}$).

2 Easy estimation

We first estimate the upper bound of maximal value of $|\mathfrak{B}|$.

For each $(i, j) \in X = Z_n \times Z_n$, let $\mathfrak{B}_{(i,j)} \subset \mathfrak{B}$ be the subset of the blocks B with $(i, j) \in B$. Since $B \cap G_i = \{(i, j)\}$ for any block $B \in \mathfrak{B}_{(i,j)}$ from Condition(C2), and since $B \cap B' = \{(i, j)\}$ for each pair of distinct blocks $B, B' \in \mathfrak{B}_{(i,j)}$ from Condition(C3), it follows

$$\left| \bigcup_{B \in \mathfrak{B}_{(i,j)}} B \right| = |\mathfrak{B}_{(i,j)}| \cdot (n-1) \leq |X| - |G_i| = |Z_n|^2 - |Z_n| = n(n-1)$$

from $\bigcup_{B \in \mathfrak{B}_{(i,j)}} B \subset X$. Thus we have

$$|\mathfrak{B}_{(i,j)}| \leq \frac{n(n-1)}{n-1} = n.$$

Each block $B \in \mathfrak{B}$ belongs to exactly n subsets $\mathfrak{B}_{(i,j)} \subset \mathfrak{B}$ with $(i,j) \in B$. It gives

$$n \cdot |\mathfrak{B}| = \sum_{(i,j) \in X} |\mathfrak{B}_{(i,j)}| \leq n^2 \cdot n,$$

hence

$$|\mathfrak{B}| \leq n^2.$$

3 Construction of the set \mathfrak{B}

This section treats the case $n = p^d$ for prime p . We will construct the block set \mathfrak{B} with $|\mathfrak{B}| = n^2$ satisfying Conditions(C1), (C2) and (C3).

Let \mathbb{F}_p be the finite field of characteristic p , and $V = \mathbb{F}_p^d$ the vector space over \mathbb{F}_p . In the case $n = p^d$, we have the one-to-one correspondence from V to Z_n defined by

$$wt(\mathbf{a}) = a_0 + a_1p + \cdots + a_{d-1}p^{d-1} = \sum_{k=0}^{d-1} a_k p^k \in Z_n$$

for any vector $\mathbf{a} \in V$, where a_k is the k -th element of the vector \mathbf{a} . Consider the d -dimensional matrix $A(\mathbf{a})$ determined by $\mathbf{a} \in V$. Define the block

$$B(\mathbf{a}, \mathbf{b}) = \{ (wt(\mathbf{r}), wt(A(\mathbf{a})\mathbf{r} + \mathbf{b})) \mid \mathbf{r} \in V \} \subset X = Z_n \times Z_n$$

for $\mathbf{a}, \mathbf{b} \in V$. Since

$$(wt(\mathbf{r}), wt(A(\mathbf{a})\mathbf{r} + \mathbf{b})) \neq (wt(\mathbf{r}'), wt(A(\mathbf{a})\mathbf{r}' + \mathbf{b}))$$

for $\mathbf{r} \neq \mathbf{r}'$, we have

$$|B(\mathbf{a}, \mathbf{b})| = |V| = p^d = n \tag{1}$$

for any $\mathbf{a}, \mathbf{b} \in V$.

From now on, we assume that the following two conditions hold:

(A1) each element of the matrix $A(\mathbf{a})$ are linear in $\mathbf{a} \in V$:

$$A(\mathbf{a} + \mathbf{a}') = A(\mathbf{a}) + A(\mathbf{a}') \quad \text{for any } \mathbf{a}, \mathbf{a}' \in V,$$

(A2) $A(\mathbf{a})$ is invertible for any non-zero vector $\mathbf{a} \in V$, $\mathbf{a} \neq \mathbf{o}$.

Under the above assumption, we consider the intersection of these blocks $B(\mathbf{a}, \mathbf{b})$ and the groups $G_i \in \mathfrak{G}$. We have to treat two cases:

(a) $B(\mathbf{a}, \mathbf{b}) \cap B(\mathbf{a}', \mathbf{b}')$, and

(b) $B(\mathbf{a}, \mathbf{b}) \cap G_i$.

Case (a): If the intersection $B(\mathbf{a}, \mathbf{b}) \cap B(\mathbf{a}', \mathbf{b}')$ is non-empty, there exist $\mathbf{r}, \mathbf{r}' \in V$ such that

$$(wt(\mathbf{r}), wt(A(\mathbf{a})\mathbf{r} + \mathbf{b})) = (wt(\mathbf{r}'), wt(A(\mathbf{a}')\mathbf{r}' + \mathbf{b}')).$$

It follows that

$$\begin{aligned} \mathbf{r} &= \mathbf{r}', \\ A(\mathbf{a})\mathbf{r} + \mathbf{b} &= A(\mathbf{a}')\mathbf{r}' + \mathbf{b}', \end{aligned}$$

and therefore

$$A(\mathbf{a} - \mathbf{a}')\mathbf{r} = \mathbf{b}' - \mathbf{b}$$

from the condition (A1). In the case $\mathbf{a} = \mathbf{a}'$, it must be $\mathbf{b} = \mathbf{b}'$ hence $B(\mathbf{a}, \mathbf{b}) = B(\mathbf{a}', \mathbf{b}')$. Otherwise, from the condition (A2), the vector $\mathbf{r} = \mathbf{r}' \in V$ is uniquely determined by $\mathbf{a}, \mathbf{b}, \mathbf{a}'\mathbf{b}' \in V$. Therefore we have $|B(\mathbf{a}, \mathbf{b}) \cap B(\mathbf{a}', \mathbf{b}')| = 0$ or 1 for different pairs $(\mathbf{a}, \mathbf{b}) \neq (\mathbf{a}', \mathbf{b}')$.

Case (b): If the intersection $B(\mathbf{a}, \mathbf{b}) \cap G_i$ is non-empty, there exist $\mathbf{r} \in V$ and $j \in Z_n$ such that

$$(wt(\mathbf{r}), wt(A(\mathbf{a})\mathbf{r} + \mathbf{b})) = (i, j). \quad (2)$$

It follows that

$$\begin{aligned} wt(\mathbf{r}) &= i, \\ wt(A(\mathbf{a})\mathbf{r} + \mathbf{b}) &= j, \end{aligned}$$

and therefore $\mathbf{r} \in V$ and $j \in Z_n$ are uniquely determined by $\mathbf{a}, \mathbf{b} \in V$ and $i \in Z_n$. Hence we have $|B(\mathbf{a}, \mathbf{b}) \cap G_i| = 1$ for any $\mathbf{a}, \mathbf{b} \in V$ and for any $i \in Z_n$.

Let $\mathfrak{B} = \{B(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in V\}$, then we can see that this satisfies the three conditions (C1), (C2), (C3). Indeed, the equality (1) gives

$$(C1) \quad |B| = n \text{ for any block } B = B(\mathbf{a}, \mathbf{b}) \in \mathfrak{B},$$

and the argument above obtains that

$$(C2) \quad |B \cap G_i| = 1 \text{ for any block } B = B(\mathbf{a}, \mathbf{b}) \in \mathfrak{B} \text{ and for any group } G_i \in \mathfrak{G}, \quad \text{and}$$

$$(C3) \quad |B \cap B'| \leq 1 \text{ for any different blocks } B = B(\mathbf{a}, \mathbf{b}), B' = B(\mathbf{a}', \mathbf{b}') \in \mathfrak{B}.$$

Then the block set \mathfrak{B} has the order

$$|\mathfrak{B}| = |\{B(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in V\}| = |V \times V| = n^2,$$

which is the desired one attaining the upper bound of $|\mathfrak{B}|$. Consequently, the answer of the question in the head of this paper is $n + 1$ times if $n = p^d$ the power of prime.

The following section will confirm the existence of the matrix $A(\mathbf{a}) \in M_e(\mathbb{F}_p)$ satisfying the conditions (A1), (A2)

4 A linear representation of $\mathbb{F}_p[x]/(h)$

Let $\mathbb{F}_p[x]$ be the polynomial ring with coefficients in the prime field \mathbb{F}_p of positive characteristic p , and let $\mathbb{F}_p[x]/(h)$ be the residue ring for a monic polynomial $h \in \mathbb{F}_p[x]$ of degree d . We here give a linear representation $\Psi : \mathbb{F}_p[x]/(h) \rightarrow M_d(\mathbb{F}_p)$ explicitly, and show the following theorem.

Theorem.

There is a ring homomorphism $\Psi : \mathbb{F}_p[x]/(h) \rightarrow M_d(\mathbb{F}_p)$ for any monic polynomial $h \in \mathbb{F}_p[x]$. In particular, in the case that h is irreducible, each image $\Psi(f)$ is invertible for $f \neq 0 \in \mathbb{F}_p[x]/(h)$.

Since there exists an irreducible polynomial $h \in \mathbb{F}_p[x]$ of any degree d as is known (for example [2]), and since any vector $\mathbf{a} = (a_i) \in \mathbb{F}_p^d$ can be correspond to the polynomial $f_{\mathbf{a}} = \sum_{k=0}^{d-1} a_k x^k \in \mathbb{F}[x]/(h)$ modulo h , there is the matrix $A(\mathbf{a}) = \Psi(f_{\mathbf{a}}) \in M_d(\mathbb{F})$ which is invertible for $\mathbf{a} \neq \mathbf{o}$. Moreover these matrices satisfy that $A(\mathbf{a} + \mathbf{b}) = A(\mathbf{a}) + A(\mathbf{b})$ for any $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^d$. Thus we obtain that the matrix $A(\mathbf{a}) \in M_d(\mathbb{F}_p)$ satisfying (A1) and (A2) in the previous section for any non-zero vector $\mathbf{a} \in \mathbb{F}_p^d$, and consequently the code set $C_0 \subset Z_{n^2}$ hold $\#C_0 = n^2 + n$. This proves our main result.

In the following, we prove the above theorem.

Proof of Theorem.

Let the monic polynomial $h \in \mathbb{F}_p[x]$ of degree d be

$$h = x^d + p_{d-1}x^{d-1} + \cdots + p_1x + p_0 = x^d + \sum_{k=0}^{d-1} p_k x^k$$

with $p_i \in \mathbb{F}_p$ ($i \in Z_d$). Denoting

$$x^{d+j} \equiv \sum_{k=0}^{d-1} p_{j,k} x^k \pmod{h} \quad (3)$$

in $\mathbb{F}_p[x]/(h)$, we have

$$x^{d+j+1} = x^{d+j}x \equiv \sum_{k=0}^{d-1} p_{j,k} x^{k+1} \equiv p_{j,d-1}p_{0,0} + \sum_{k=1}^{d-1} (p_{j,k-1} + p_{j,d-1}p_{0,k})x^k.$$

and have the inductive relation

$$p_{0,k} = -p_k \quad (k \in Z_d), \quad (4)$$

and

$$p_{j,k} = p_{j-1,k-1} + p_{j-1,d-1}p_{0,k} \quad (j, k \in Z_d, j > 0), \quad (5)$$

with $p_{j,k} = 0$ of $j < 0$ or $k < 0$ for convenience.

For any polynomial $f = \sum_{k=0}^{d-1} a_k x^k$, $g = \sum_{k=0}^{d-1} b_k x^k \in \mathbb{F}_p[x]$ (here also $a_k = b_k = 0$ with $k < 0$ or $k > d-1$ for convenience), it follows from (3) that

$$\begin{aligned} fg &= \sum_{k=0}^{2d-2} \sum_{l=0}^k a_l b_{k-l} x^k = \sum_{k=0}^{d-1} \sum_{l=0}^k a_l b_{k-l} x^k + \sum_{k=d}^{2d-2} \sum_{l=0}^k a_l b_{k-l} x^k \\ &= \sum_{k=0}^{d-1} \sum_{l=0}^k a_l b_{k-l} x^k + \sum_{j=0}^{d-2} \sum_{l=j+1}^{d-1} a_l b_{d+j-l} x^{d+j} \\ &= \sum_{k=0}^{d-1} \tilde{c}_k x^k + \sum_{j=0}^{d-2} \tilde{c}_{d+j} x^{d+j} \\ &= \sum_{k=0}^{d-1} \left(\tilde{c}_k + \sum_{j=0}^{d-2} \tilde{c}_{d+j} p_{j,k} \right) x^k \\ &= \sum_{k=0}^{d-1} c_k x^k, \end{aligned}$$

where \tilde{c}_k denotes the coefficient of the term of degree k in $fg \in \mathbb{F}_p[x]$:

$$\tilde{c}_k = \sum_{l=0}^k a_l b_{k-l} \quad (k \in Z_d), \quad \tilde{c}_{d+k} = \sum_{l=k+1}^{d-1} a_l b_{d+k-l} \quad (k \in Z_{d-1}), \quad (6)$$

and c_k denotes the coefficient of the term of degree k in $fg \in \mathbb{F}_p[x]/(h)$:

$$c_k = \tilde{c}_k + \sum_{j=0}^{d-2} \tilde{c}_{d+j} p_{j,k} \quad (k \in Z_d). \quad (7)$$

We now construct the morphism $\Psi : \mathbb{F}_p[x]/(h) \rightarrow M_d(\mathbb{F}_p)$ as follows. For any polynomial $f = \sum_{k=0}^{d-1} a_k x^k \in \mathbb{F}_p[x]/(h)$ with $\deg f = d-1$, the (i, j) -element $\alpha_{i,j}$ in the matrix $\Psi(f) \in M_d(\mathbb{F}_p)$ is defined by

$$\alpha_{0,j} = a_j, \quad (8)$$

$$\alpha_{i,j} = a_{j-i} \delta_{j \geq i} + \sum_{m=0}^{i-1} a_{d-(i-m)} p_{m,j} \quad (i > 0), \quad (9)$$

where

$$\delta_{j \geq i} = \begin{cases} 1 & (j \geq i) \\ 0 & (j < i). \end{cases}$$

Under the notation above, for $i > 0$, we have the inductive relation

$$\alpha_{i,j} = \alpha_{i-1,j-1} + \alpha_{i-1,d-1} p_{0,j} \quad (10)$$

because

$$\begin{aligned} \alpha_{i,j} &= a_{j-i} \delta_{j \geq i} + \sum_{m=0}^{i-1} a_{d-(i-m)} p_{m,j} \\ &= a_{j-i} \delta_{j \geq i} + a_{d-i} p_{0,j} + \sum_{m=1}^{i-1} a_{d-(i-m)} (p_{m-1,j-1} + p_{m-1,d-1} p_{0,j}) \\ &= a_{j-i} \delta_{j \geq i} + \sum_{m=1}^{i-1} a_{d-(i-m)} p_{m-1,j-1} + \left(a_{d-i} + \sum_{m=1}^{i-1} a_{d-(i-m)} p_{m-1,d-1} \right) p_{0,j} \\ &= a_{(j-1)-(i-1)} \delta_{(j-1) \geq (i-1)} + \sum_{m=0}^{(i-1)-1} a_{d-((i-1)-m)} p_{m,j-1} \\ &\quad + \left(a_{(d-1)-(i-1)} \delta_{(d-1) \geq (i-1)} + \sum_{m=0}^{(i-1)-1} a_{d-((i-1)-m)} p_{m,d-1} \right) p_{0,j} \\ &= \alpha_{i-1,j-1} + \alpha_{i-1,d-1} p_{0,j} \end{aligned}$$

from (5), (9) and (10).

We will show that the morphism $\Psi : \mathbb{F}_p[x]/(h) \rightarrow M_d(\mathbb{F}_p)$ is the ring homomorphism, that is, that $\Psi(fg) = \Psi(f) \Psi(g)$ and $\Psi(fg) = \Psi(f) \Psi(g)$ hold. One can derive the first relation easily, so one has only to treat the second one. For any $f = \sum_{k=0}^{d-1} a_k x^k, g = \sum_{k=0}^{d-1} b_k x^k \in \mathbb{F}_p[x]/(h)$,

denoting the (i, j) -elements in $\Psi(f)$, $\Psi(g)$ and $\Psi(fg)$ by $\alpha_{i,j}$, $\beta_{i,j}$ and $\gamma_{i,j}$, respectively, we have the relations

$$\alpha_{0,j} = a_j, \quad \alpha_{i,j} = a_{j-i}\delta_{j \geq i} + \sum_{m=0}^{i-1} a_{d-(i-m)}p_{m,j} = \alpha_{i-1,j-1} + \alpha_{i-1,d-1}p_{0,j} \quad (i > 0), \quad (11)$$

$$\beta_{0,j} = b_j, \quad \beta_{i,j} = b_{j-i}\delta_{j \geq i} + \sum_{m=0}^{i-1} b_{d-(i-m)}p_{m,j} = \beta_{i-1,j-1} + \beta_{i-1,d-1}p_{0,j} \quad (i > 0), \quad (12)$$

$$\gamma_{0,j} = c_j, \quad \gamma_{i,j} = c_{j-i}\delta_{j \geq i} + \sum_{m=0}^{i-1} c_{d-(i-m)}p_{m,j} = \gamma_{i-1,j-1} + \gamma_{i-1,d-1}p_{0,j} \quad (i > 0) \quad (13)$$

from (8), (9) and (10). On the other hand, the (i, j) -element $\gamma'_{i,j}$ in the matrix $\Psi(f)\Psi(g)$ is given by $\gamma'_{i,j} = \sum_{k=0}^{d-1} \alpha_{i,k}\beta_{k,j}$. In the case $i = 0$, we have

$$\begin{aligned} \gamma'_{0,j} &= \sum_{k=0}^{d-1} \alpha_{0,k}\beta_{k,j} \\ &= \sum_{k=0}^{d-1} a_k \left(b_{j-k}\delta_{j \geq k} + \sum_{m=0}^{k-1} b_{d-(k-m)}p_{m,j} \right) \\ &= \sum_{k=0}^j a_k b_{j-k} + \sum_{k=1}^{d-1} \sum_{m=0}^{k-1} a_k b_{d-(k-m)}p_{m,j} \\ &= \sum_{k=0}^j a_k b_{j-k} + \sum_{m=0}^{d-2} \sum_{k=m+1}^{d-1} a_k b_{d-(k-m)}p_{m,j} \\ &= \tilde{c}_j + \sum_{m=0}^{d-2} \tilde{c}_{d+m}p_{m,j} = c_j = \gamma_{0,j} \end{aligned}$$

from (6) and (7). In the case $i > 0$, it follows from (11) and (12) that

$$\begin{aligned} \gamma'_{i,j} &= \sum_{k=0}^{d-1} \alpha_{i,k}\beta_{k,j} \\ &= \sum_{k=1}^{d-1} \alpha_{i-1,k-1}\beta_{k,j} + \sum_{k=0}^{d-1} \alpha_{i-1,d-1}p_{0,k}\beta_{k,j} \\ &= \sum_{k=1}^{d-1} \alpha_{i-1,k-1}\beta_{k-1,j-1} + \sum_{k=1}^{d-1} \alpha_{i-1,k-1}\beta_{k-1,d-1}p_{0,j} + \sum_{k=0}^{d-1} \alpha_{i-1,d-1}p_{0,k}\beta_{k,j} \\ &= \sum_{k=0}^{d-2} \alpha_{i-1,k}\beta_{k,j-1} + \sum_{k=0}^{d-2} \alpha_{i-1,k}\beta_{k,d-1}p_{0,j} + \sum_{k=0}^{d-1} \alpha_{i-1,d-1}p_{0,k}\beta_{k,j}. \end{aligned} \quad (14)$$

If the relation

$$\sum_{k=0}^{d-1} \beta_{k,j}p_{0,k} = \beta_{d-1,j-1} + \beta_{d-1,d-1}p_{0,j}. \quad (15)$$

holds, it follows from (14) that

$$\gamma'_{i,j} = \gamma'_{i-1,j-1} + \gamma'_{i-1,d-1}p_{0,j}$$

and from (13) that

$$\gamma'_{i,j} = \gamma_{i,j}$$

inductively in i , consequently $\Psi(f)\Psi(g) = \Psi(fg)$.

After here, we will assure that the relation (15) holds. It follows from (11) and (12) that

$$\begin{aligned} \sum_{k=0}^{d-1} \beta_{k,j} p_{0,k} &= \beta_{0,j} p_{0,0} + \sum_{k=1}^{d-1} \beta_{k-1,j-1} p_{0,k} + \sum_{k=1}^{d-1} \beta_{k-1,d-1} p_{0,j} p_{0,k} \\ &= \beta_{0,j} p_{0,0} + \sum_{k=1}^{d-1} \beta_{k-1,j-1} p_{0,k} + \sum_{k=1}^{d-1} (\beta_{k,k} - \beta_{k-1,k-1}) p_{0,j} \\ &= \sum_{k=1}^{d-1} \beta_{k-1,j-1} p_{0,k} + \beta_{0,j} p_{0,0} + \beta_{d-1,d-1} p_{0,j} - \beta_{0,0} p_{0,j}, \end{aligned}$$

and that

$$\begin{aligned} \sum_{k=1}^{d-1} \beta_{k-1,j-1} p_{0,k} &= \beta_{0,j-1} p_{0,1} + \sum_{k=2}^{d-1} \beta_{k-2,j-2} p_{0,k} + \sum_{k=2}^{d-1} \beta_{k-2,d-1} p_{0,j-1} p_{0,k} \\ &= \beta_{0,j-1} p_{0,1} + \sum_{k=2}^{d-1} \beta_{k-2,j-2} p_{0,k} + \sum_{k=2}^{d-1} (\beta_{k-1,k} - \beta_{k-2,k-1}) p_{0,j-1} \\ &= \sum_{k=2}^{d-1} \beta_{k-2,j-2} p_{0,k} + \beta_{0,j-1} p_{0,1} + \beta_{d-2,d-1} p_{0,j-1} - \beta_{0,1} p_{0,j-1}, \end{aligned}$$

and similarly that

$$\sum_{k=j-1}^{d-1} \beta_{k-(j-1),1} p_{0,k} = \sum_{k=j}^{d-1} \beta_{k-j,0} p_{0,k} + \beta_{0,1} p_{0,j-1} + \beta_{d-j,d-1} p_{0,1} - \beta_{0,j-1} p_{0,1}.$$

We get consequently that

$$\begin{aligned} \sum_{k=0}^{d-1} \beta_{k,j} p_{0,k} &= \sum_{k=j}^{d-1} \beta_{k-j,0} p_{0,k} + \beta_{0,j} p_{0,0} + \sum_{l=0}^{j-1} \beta_{d-1-l,d-1} p_{0,j-l} - \beta_{0,0} p_{0,j} \\ &= \sum_{k=j}^{d-1} \beta_{k-j,0} p_{0,k} + \beta_{0,j} p_{0,0} + \sum_{l=1}^{j-1} (\beta_{d-l,j-l} - \beta_{d-1-l,j-l-1}) + \beta_{d-1,d-1} p_{0,j} - \beta_{0,0} p_{0,j} \\ &= \sum_{k=j}^{d-1} \beta_{k-j,0} p_{0,k} + \beta_{0,j} p_{0,0} + \beta_{d-1,j-1} - \beta_{d-j,0} + \beta_{d-1,d-1} p_{0,j} - \beta_{0,0} p_{0,j} \\ &= \sum_{k=j+1}^{d-1} \beta_{k-j,0} p_{0,k} + \beta_{0,j} p_{0,0} + \beta_{d-1,j-1} - \beta_{d-j,0} + \beta_{d-1,d-1} p_{0,j} \\ &= \sum_{k=j+1}^{d-1} \beta_{k-j-1,d-1} p_{0,0} p_{0,k} + \beta_{0,j} p_{0,0} + \beta_{d-1,j-1} - \beta_{d-j,0} + \beta_{d-1,d-1} p_{0,j} \\ &= \sum_{k=j+1}^{d-1} (\beta_{k-j,k} - \beta_{k-j-1,k-1}) p_{0,0} + \beta_{0,j} p_{0,0} + \beta_{d-1,j-1} - \beta_{d-j,0} + \beta_{d-1,d-1} p_{0,j} \\ &= \beta_{d-1-j,d-1} p_{0,0} - \beta_{0,j} p_{0,0} + \beta_{0,j} p_{0,0} + \beta_{d-1,j-1} - \beta_{d-j,0} + \beta_{d-1,d-1} p_{0,j} \\ &= \beta_{d-1-j,d-1} p_{0,0} + \beta_{d-1,j-1} - \beta_{d-j,0} + \beta_{d-1,d-1} p_{0,j} \\ &= \beta_{d-1,j-1} + \beta_{d-1,d-1} p_{0,j}, \end{aligned}$$

because $\beta_{d-j,0} = \beta_{d-1-j,d-1}p_{0,0}$ by (12). This is the desired relation (15), and hence the morphism $\Psi : \mathbb{F}_p[x]/(h) \rightarrow M_d(\mathbb{F}_p)$ is a ring homomorphism.

Reference

- [Bos] Bose, R. C. : On the applications of properties of Galois fields to the problem of construction of hypergraelatin square, *Sankhya*, **3** (1938), 323–338.
- [CD] Colbourn, C. J., Dinitz, J. H. : Mutually orthogonal latin squares: a brief survey of constructions, *Journal of statistical planning and inference*, **95** (2001), 9–48.
- [Eul] Euler, L. : Recherches sur une nouvelle espèce de quarrés magiques, *Verh. Zeeuw. Gen. Welten. Vlissengen*, **9** (1782), 85–239.
- [Moo] Moore, E. H. : Tactical memoranda I–III, *Amer. J. Math.*, **18** (1896), 264–236.
- [Tak] Takeuchi, K., Grouping Problem (in Japanese), *Journal of the School of Education, Sugiyama Jogakuen University*, **6** (2013), 21–27