E0 221 Discrete Structures / August-December 2013

(ME, MSc, Ph. D. Programmes)

Download from : `http://www.math.iisc.ernet.in/patil/courses/courses/Current Courses/...`

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** `dppatil@csa.iisc.ernet.in` / `patil@math.iisc.ernet.in`

Lectures : Monday and Wednesday ; 10:00–11:30 **Venue:** CSA, Lecture Hall (Room No. 117)

TAs/Corrections by : **Akanksha Agrawal** (`akanksha.agrawal@csa.iisc.ernet.in`)
Palash Dey (`palash@csa.iisc.ernet.in`) / **Govind Sharma** (`govindjsk@csa.iisc.ernet.in`)
Sayantan Mukheriee (`sayantan.mukherjee@csa.iisc.ernet.in`)

Quizzes : During Wednesday, Lectures on **Aug 28; Sept 18; (Monday) Oct 14; Oct 30;** **Time :** 10:00 -10:15

1-st Midterm : Sunday, September 15, 2013; 14:00 -16:30 **2-nd Midterm :** Sunday, October 20, 2013; 14:00 -16:30

Final Examination : Saturday, December 07, 2013, 14:00 -17:00

Evaluation Weightage : Quizzes (Four) + Midterms (Two) : 50% **Final Examination :** 50%

Range of Marks for Grades (Total 100 Marks)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	76–90	61–75	46–60	35–45	< 35

6. Finite Sets — Elementary Counting Techniques

- **Solution of the Exercise *6.8 carries 10 Bonus Points.**
- **Recommended to read the Exercises ^{R}6.9 and ^{R}6.10.**

6.1 **(a)** (Tower of Hanoi[1]) The puzzle consists of n disks of decreasing diameter placed on a pole. There are two other poles. The problem is to move the entire pile to another pole by moving one disk at a time to any other pole, except that no disk may be placed on top of a smaller disk.

Find a formula for the least number of moves needed to move n disks from one pole to another, and prove the formula by induction. (**Hint :** Let T_n be the minimum number of moves needed to solve the puzzle with n disks. Then note that $\mathrm{T}_0 = 0$, $\mathrm{T}_1 = 1$, $\mathrm{T}_2 = 3$, $\mathrm{T}_3 = 7$ and $\mathrm{T}_4 = 15$. Moreover, (check!) the recurrence relation $\mathrm{T}_n = 2\cdot\mathrm{T}_{n-1}+1$ for $n > 0$. Conclude that $\mathrm{T}_n = 2^n - 1$.)

(b) Let X, Y be finite sets and $Z := X \times Y$. For $x \in X$, let $P_x := \{y \in Y \mid (x,y) \in Z\}$ and for $y \in Y$, let $Q_y := \{x \in X \mid (x,y) \in Z\}$. Show that $\sum_{x\in X} |P_x| = \sum_{y\in Y} |Q_y|$. (**Hint :** Note that $Z = \biguplus_{x\in X} P_x = \biguplus_{y\in Y} Q_y$.)

6.2 Let X be a finite set with n elements.

(a) The number of subsets of X is 2^n. (**Hint :** The map $\mathfrak{P}(X) \to \{0,1\}^X$, $A \mapsto e_A$ is bijective, where $e_A : X \to \{0,1\}$ denote the indicator function of the subset A, see also Ex. Set 2, T2.26.)

(b) If $n \in \mathbb{N}^*$, then the number of subsets of X with an even number of elements is equal to the number of subsets of X with an odd number of elements. Moreover, this number is equal to 2^{n-1}. (**Hint :** Let $a \in X$. The map defined by $A \mapsto A \cup \{a\}$, if $a \notin A$, resp. $A \smallsetminus \{a\}$, if $a \in A$, is a bijective map from the set $\mathfrak{P}_{\text{even}}(X)$ of all subsets of X with an even number of elements onto the set $\mathfrak{P}_{\text{odd}}(X)$ of all subsets of X with an odd number of elements.)

[1] The French mathematician François Edouard Anatole Lucas (1842-1891) invented the Tower of Hanoi puzzle and other mathematical recreations. The Tower of Hanoi puzzle appeared in 1883 under the name of *M. Claus*. Notice that *Claus* is an anagram of Lucas! His four volume work on recreational mathematics *Récréations mathématiques* (1882-94) has become a classic. He is best known for his results in number theory. He studied the Fibonacci sequence and devised the test for Mersenne primes still used today.

(c) For $n \in \mathbb{N}$, prove that : $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}=2^n$. (**Hint :** For $k \in \{0,1,\ldots,n\}$, let $\mathfrak{P}_k(\{1,\ldots,n\})$ denote the set of all subsets of $\{1,\ldots,n\}$ of cardinality k. Then $\#\mathfrak{P}_k(\{1,\ldots,n\})=\binom{n}{k}$ and $\mathfrak{P}(\{1,\ldots,n\})=\biguplus_{k=0}^{n}\mathfrak{P}_k(\{1,\ldots,n\})$. Now, use part (a).)

(d) For $n \in \mathbb{N}^*$, prove that : $\binom{n}{0}-\binom{n}{1}+\cdots+(-1)^n\binom{n}{n}=0$. (**Hint :** Use part (b) or $(1-1)^n=0$.)

(e) Prove that $\sum_{k=0}^{n}\binom{2n+1}{2k}=4^n=\sum_{k=0}^{n}\binom{2n+1}{2k+1}$ for $n \in \mathbb{N}$ and $\sum_{k=0}^{n}\binom{2n}{2k}=\frac{4^n}{2}=\sum_{k=0}^{n-1}\binom{2n}{2k+1}$ for $n \in \mathbb{N}^*$. (**Hint :** Use part (b).)

(f) Let Y be a k-element subset of X. Then the number of m-element subsets of X which contain Y is $\binom{n-k}{m-k}$.

(g) For natural numbers m,n with $m \le n$, show that $\sum_{k=0}^{m}\binom{n}{k}\binom{n-k}{m-k}=2^m\binom{n}{m}$. (**Hint :** Compute the sum of all numbers in the part (f), where Y runs through all k-element subsets of X in two different ways or use the formula $\binom{n}{k}\binom{n-k}{m-k}=\binom{n}{m}\binom{m}{k}$.)

(h) For $m,n,k \in \mathbb{N}$, prove that $\displaystyle\binom{m+n}{k}=\binom{m}{0}\binom{n}{k}+\binom{m}{1}\binom{n}{k-1}+\cdots+\binom{m}{k}\binom{n}{0}$. In particular, $\binom{2n}{n}=\binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n}^2$ for $n \in \mathbb{N}$. (**Hint :** Let X,Y be disjoint sets with $|X|=m$, $|Y|=n$. The assignment $A \mapsto (A\cap X, A\cap Y)$ defines a bijective map $\mathfrak{P}(X\cup Y)\to\mathfrak{P}(X)\times\mathfrak{P}(Y)$.)

(i) What is the cardinality of the set $\mathfrak{P}_{\ge n+1}(\{1,\ldots,2n+1\})$ of subsets of $\{1,\ldots,2n+1\}$ of cardinality $\ge n+1$? (see also Exercise 6.5-(d), parts (e) and (d) above.)

(j) Let $r,k,n,m \in \mathbb{N}$.

(i) If $r \le k \le n$, then $\binom{n}{k}\binom{k}{r}=\binom{n}{r}\binom{n-r}{k-r}$. (**Hint :** Just compute both sides!. **Variant :** Suppose from n objects we choose k and put a white tag on the selected objects. Then out of these k objects we select r objects and put a black tag on those selected. This is equivalent to selecting r objects (and putting white and a black tag on each) and then selecting $k-r$ objects from the remaining $n-r$ putting a white tag on the the selected objects.)

(ii) If $m \le k$, then $\sum_{j=0}^{k-m}(-1)^j\binom{m+j}{m}\binom{k}{m+j}=0$.

(**Hint :** $\sum_{j=0}^{k-m}(-1)^j\binom{m+j}{m}\binom{k}{m+j}=\sum_{j=0}^{k-m}(-1)^j\binom{k}{m}\binom{k-m}{j}=\binom{k}{m}\sum_{j=0}^{k-m}(-1)^j\binom{k-m}{j}=0$ by Exercise 6.2-(d).)

(iii) $\sum_{k=0}^{n}k\cdot(k!)=(n+1)!-1$. (**Hint :** Prove by induction on n.)

(iv) $\sum_{k=m}^{n}\binom{k}{m}=\binom{n+1}{m+1}$, $m \in \mathbb{N}$, $m \le n$. (**Hint :** Prove by induction on n.)

6.3 Let X be a finite set with n elements.

(a) Prove that the number of pairs (X_1,X_2) in $\mathfrak{P}(X)\times\mathfrak{P}(X)$ with $X_1\cap X_2=\emptyset$ is 3^n. More generally : The number of m–tuples $(X_1,\ldots,X_m)$ of pairwise disjoint subsets $X_1,\ldots,X_m\subseteq X$ is equal $(m+1)^n$.

(b) For $n,r \in \mathbb{N}$, prove that $\sum_m\binom{n}{m}=r^n$, where m run through the set of all r-tuples $(m_1,\ldots,m_r)\in\mathbb{N}^r$ of natural numbers with $m_1+\cdots+m_r=n$. (**Hint :** Use $r^n=(1+\cdots+1)^n$ or the part (a).)

6.4 Let X be a finite set with m elements.

(a) Let p_m denote the number of permutations of X which do not have fixed points and let $s_m=m!$ be the number of all permutations of X. Show that :

$$\frac{p_m}{s_m}=\frac{1}{0!}-\frac{1}{1!}+\cdots+(-1)^m\cdot\frac{1}{m!}\,.$$

(**Hint :** Let $X=\{x_1,\ldots,x_m\}$. Set $X_i:=\{\sigma\in\mathfrak{S}(X):\sigma(x_i)=x_i\}$ and compute $s_m-p_m=|\bigcup_{i=1}^{m}X_i|$ using the Sieve formula in T6.1. – **Remark :** Note that by definition $e:=\lim_{n\to\infty}(1+\frac{1}{n})^n=2.71828182845904523536\ldots$ is the *Euler's number* which is base of the natural logarithm and $\lim_{m\to\infty}(p_m/s_m)=e^{-1}$.)

(b) For every $0\le r\le m$, show that the number of permutations of X with exactly r fixed points is $\displaystyle\binom{m}{r}p_{m-r}$. (**Hint :** For $\sigma\in\mathfrak{F}_r(X):=\{\sigma\in\mathfrak{S}(X)\mid\#\mathrm{Fix}(\sigma)=r\}$, let $\mathrm{Supp}\,\sigma:=(X\setminus\mathrm{Fix}\,\sigma)$ and

$f_\sigma : \operatorname{Supp}\sigma \to \{1,\ldots,m-r\}$ be a (fixed) bijection and let $\rho_\sigma := f_\sigma \circ (\sigma_{|\operatorname{Supp}\sigma}) \circ (f_\sigma)^{-1} \in \mathfrak{S}_{m-r}$. With this show that the map $\mathfrak{F}_r(X) \to \mathfrak{P}_r(X) \times \{\rho \in \mathfrak{S}_{m-r} \mid \operatorname{Fix}\rho = \emptyset\}$ defined by $\sigma \mapsto (\operatorname{Fix}\sigma\,,\,\rho_\sigma)$ is bijective!)

(c) Let X be a finite set with m elements and let Y be a finite set with n elements. The number of surjective maps from X in Y is

$$n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots + (-1)^n\binom{n}{n}(n-n)^m\,.$$

(**Hint :** Let $Y = \{y_1,\ldots,y_n\}$. Set $P_i := \{f \in Y^X : y_i \notin \ \operatorname{im} f\}$ and compute the number $|\bigcup_{i=1}^n P_i|$ of non-surjective maps using the Sieve formula in T6.1.))

6.5 Let m,n be two natural numbers.

(a) Let $\mathrm{a}(m,n)$ (respectively, $\mathrm{b}(m,n)$) denote the number of m–tuples $(x_1,\ldots,x_m) \in \mathbb{N}^m$ with $x_1+\cdots+x_m \le n$ (respectively, $x_1+\cdots+x_m = n$). Show that

$$\mathrm{a}(m,n) = \binom{n+m}{m} \quad \text{and} \quad \mathrm{b}(m,n) = \binom{n+m-1}{m-1}.$$

(**Hint :** Remember to put $\binom{-1}{-1} := 1$. For $m \ge 1$, note the equalities $\mathrm{a}(m-1,n) = \mathrm{b}(m,n)$ and $\mathrm{a}(m,n) = \mathrm{a}(m,n-1) + \mathrm{a}(m-1,n)$ and then use induction on $n+m$. – **Variant :** Show that the map $(x_1,\ldots,x_m) \mapsto \{x_1+1, x_1+x_2+2,\ldots,x_1+\cdots+x_m+m\}$ maps the set of m–tuples $(x_1,\ldots,x_m) \in \mathbb{N}^m$ with $x_1+\cdots+x_m \le n$ bijectively onto the set of m–element subsets of $\{1,2,\ldots,n+m\}$.)

(b) Suppose that $m \ge 1$. Prove that the number of m–tuples $(x_1,\ldots,x_m) \in (\mathbb{N}^+)^m$ of positive natural numbers with $x_1+\cdots+x_m = n$ is $\binom{n-1}{m-1}$.

(c) Let $k \in \mathbb{N}$ with $k \le n$. Prove that the subset

$$\mathfrak{X} = \{A \in \mathfrak{P}_k(\{1,\ldots,n\}) \mid \text{if } \ a \in A, \ \text{ then } \ a+1 \notin A\}$$

of $\mathfrak{P}_k(\{1,\ldots,n\})$ has cardinality $\binom{n-k+1}{k}$.

(d) Let $X = \{x_1,\ldots,x_{2n+1}\}$, $n \in \mathbb{N}$ be a set with $2n+1$ elements. For $k = 0,1,\ldots,n$, let $\mathfrak{X}_k$ be the set of all those subsets of X of cardinality $\ge n+1$ which contain x_{n+k+1} and exactly n elements from $x_1,\ldots,x_{n+k}$, i.e.

$$\mathfrak{X}_k = \{A \in \mathfrak{P}_{\ge n+1}(X) \mid |A \cap \{x_1,\ldots x_{n+k}\}| = n \text{ and } x_{n+k+1} \in A\}\,.$$

Show that $\bigcup_{k=0}^n \mathfrak{X}_k = \mathfrak{P}_{\ge n+1}(X)$ and hence deduce that $\sum_{k=0}^n 2^{n-k}\binom{n+k}{k} = 4^n$.

(Note that subsets of X which are elements of $\mathfrak{X}_k$ may contain some elements from $x_{n+k+2},\ldots,x_{n+1}$. See also Exercise 6.2-(e), (i).)

6.6 For $k \in \mathbb{N}^+$, a k-ary sequence is a sequence with values in a finite set with k elements (generally in the set $\{0,\ldots,k-1\}$), i.e. a k-ary sequence is an element in the set $\{0,\ldots,k-1\}^{\mathbb{N}}$. For $k = 2,3,4,5$ these sequences are also called binary, ternary, quaternary, quintnary sequences. There are exactly $k^n = |\{0,1,\ldots,k-1\}^{\{1,\ldots,n\}}|$ k-ary sequences of length n. (See also Exercise 3.4.)

(a) Find how many *palindromes*[2] of length n can be formed with an alphabet of k letters. (**Ans :** k^m if $n = 2m$ and k^{m+1} if $n = 2m+1$.)

(b) How many k-ary sequences of length n are there in which no two consecutive entries are the same? (**Ans :** $k(k-1)^{n-1}$.)

(c) How many ternary sequences of length n are there which either start with 012 or end with 012 ? (**Ans :** 0 if $n \le 2$; $2 \cdot 3^{m-3}$, if $3 \le n \le 5$; and $2 \cdot 3^{n-3} - 3^{n-6}$, if $n \ge 6$.)

(d) Show that the number of binary sequences of length n in which the digit 1 occurs even number of times is 2^{n-1}. This is also the number of binary sequences of length n in which the digit 1 occurs odd number of times. (**Hint :** Let $X := \{0,1\}^{\{1,\ldots,n\}}$ be the set of all binary sequences of length n and let

[2] A palindrome is a word which reads the same backward or forward, e. g., “MADAM”, “ANNA”.

$X_{\text{even}}(1)$ (respectively, $X_{\text{odd}}(1)$) be the set of all binary sequences of length n in which the digit 1 occurs even (respectively, odd) number of times. Then clearly $X = X_{\text{even}}(1) \uplus X_{\text{odd}}(1)$. First assume that n is odd. Then the map $f : X \to X$ defined by $f((a_1,\ldots,a_n) = (a'_1,\ldots,a'_n)$, where $a'_i = 0$ or 1 according as $a_i = 1$ or 0 for all $i = 1,\ldots n$, is a bijection. Moreover, if n is odd, then $f(X_{\text{even}}(1)) = X_{\text{odd}}(1)$ and $f(X_{\text{odd}}(1)) = X_{\text{even}}(1)$. Therefore $|X_{\text{even}}(1)| = |X_{\text{odd}}(1)|$ and $2^n = |X| = |X_{\text{even}}(1)| + |X_{\text{odd}}(1)| = 2\cdot|X_{\text{even}}(1)| = 2\cdot|X_{\text{odd}}(1)|$. Now, if n is even, then one can reduce the computation to the case when n is odd : Let $A := \{(a_1,\ldots,a_n,a_{n+1}) \in X \mid a_{n+1} = 1\}$ and $B := \{(a_1,\ldots,a_n,a_{n+1}) \in X \mid a_{n+1} = 0\}$. Then $|A| = |B| = 2^{n-1}$ and hence $X = A \uplus B$. Further, $X_{\text{even}}(1) = (A \cap X_{\text{even}}(1)) \uplus (B \cap X_{\text{even}}(1))$ and hence $|X_{\text{even}}(1)| = |(A \cap X_{\text{even}}(1))| + |(B \cap X_{\text{even}}(1))| = 2^{n-2} + 2^{n-2} = 2^{n-1}$, since $n-1$ is odd. Finally, $|X_{\text{odd}}(1)| = |X| - |X_{\text{even}}(1))| = 2^n - 2^{n-1} = 2^{n-1}$.)

(e) Show that the number of k-ary sequences of length n in which the digit 1 occurs even number of times is $\dfrac{k^n + (k-2)^n}{2}$. (**Hint :** Let $Y := \{2,3,\ldots,k-1\}^{\{1,\ldots,n\}}$ denote the set of all those k-ary sequences of length n which do not contain 0 or 1 and let $Z := X \setminus Y$. Classify the sequences in Z by their pattern, i.e., consider the equivalence classes $\sim Z_1,\ldots,Z_s$ with respect to the equivalence relation on Z. Then $|Z| = |Z_1| + \cdots + |Z_s|$. Note that by definition Z_i is the set of all k-ary sequences of length n which have the same pattern of the symbols $2,3,\ldots,k-1$ and hence $|Z_i| = 2^{n-r}$, where r is the number of places filled by the symbols $2,3,\ldots,k-1$. Now by part (a) half of these sequences have even number of 1's and this is true for all $i = 1,\ldots,s$. This proves that $|Z_{\text{even}}(1)| = \sum_{i=1}^{s} \frac{1}{2}|Z_i| = \frac{1}{2}|Z| = \frac{1}{2}(k^n - (k-2)^n)$. Therefore, since $X_{\text{even}}(1) = Y \uplus Z_{\text{even}}(1)$, we get $|X_{\text{even}}| = |Y| + |Z_{\text{even}}(1)| = (k-2)^n + \frac{1}{2}(k^n - (k-2)^n)$.)

(f) For positive natural numbers $n,k \in \mathbb{N}^+$, $k \geq 2$, prove the formula :

$$\sum_{r\in\mathbb{N}} \binom{n}{2r} (k-1)^{n-2r} = \frac{k^n + (k-2)^n}{2}.$$

(**Hint :** Follows from the part (b), since the sum on the left is the number of k-ary sequences of length n in which the digit 1 occurs even number of times.)

(g) Show that the number of k-ary sequences of length n in which both 0 and 1 occur even number of times is $\dfrac{k^n + 2(k-2)^n + (k-4)^n}{4}$, $k \geq 2$.
(**Hint :** Let 1 occur $2r$ times in a k-ary sequences of length n. Then the remaining $(k-1)$-ary sequence is of length $n-2r$. If 0 occur in an even number of times, then by part (b), there are $\dfrac{(k-1)^{n-2r} + (k-3)^{n-2r}}{2}$ such sequences. Now the assertion follows by applying the part (c) twice (once for k and then for $k-2$) and adding.)

(h) Find the number of k-ary sequences of length n in which the digit 1 occurs even number of times and the digit 0 occurs odd number of times. (**Hint :** The answer is $\dfrac{k^n - (k-4)^n}{4}$ – From the k-ary sequences of length n in which the digit 1 occur even number of times, remove the k-ary sequences of length n in which the digit 0 occur even number of times, i.e. compute

$$\sum_{r\in\mathbb{N}} \binom{n}{2r} \Big[(k-1)^{n-2r} - \frac{(k-1)^{n-2r} + (k-3)^{n-2r}}{2}\Big].)$$

6.7 Let X be a finite set with $\#X = n$ and let $m := (m_1,\ldots,m_r) \in \mathbb{N}^r$ be such that $m_1 + \cdots + m_r = n$. Show that the number of partitions $\mathfrak{p} = (X_1,\ldots,X_r)$ of X with $\#X_i = m_i$, for all $i = 1,\ldots,r$, is the polynomial coefficient $\binom{n}{m}$, i. e., $\#\mathfrak{Par}_r(X;m_1,\ldots,m_r) = \dbinom{n}{m} := \dfrac{n!}{m!} = \dfrac{n!}{m_1!\cdots m_r!}$. (**Hint :** Show that the fibres of map $\mathfrak{S}(X) \longrightarrow \mathfrak{Z} := \{\mathfrak{p} = (X_1,\ldots,X_r) \in \mathfrak{Par}_r(X) \mid |X_i| = m_i, i = 1,\ldots,r\}$ defined by $f \mapsto \mathfrak{p}(f) := (f(X_1),\ldots,f(X_r))$ have the same cardinality $= m! := m_1!\cdots m_r!$. Now use the Shepherd-rule 2.B.12.)

***6.8** Let X be a set. A permutation $\iota : X \to X$ of X is called an involution or a reflection, if ι is its own inverse, i. e., if $\iota = \iota^{-1}$, or equivalently, – if $\iota^2 = \text{id}_X$. The set

$S(\iota) := \operatorname{Fix}\iota = \{x \in X \mid \iota(x) = x\}$ of the fixed points of ι is also called the mirror of ι. In the following, let ι be a reflection of X. Let $\operatorname{Inv}(X)$ denote the set of all involutions of a set X.

(a) The set $\mathfrak{p}(\iota) := \big\{\{x,\iota(x)\} \bigm| x \in X \setminus S(\iota)\big\}$ is a partition of $X \setminus S(\iota)$ into 2-element subsets. The map $\iota \mapsto \big(S(\iota), \mathfrak{p}(\iota)\big)$ is a bijection from the set $\operatorname{Inv}(X)$ of all involutions of X onto the set of ordered pairs $\{(S,\mathfrak{p}) \mid S \in \mathfrak{P}(X)$ and $\mathfrak{p} \in \mathfrak{Par}((X \setminus S);2)\}$.

(**Hint :** Note that for a set Y, the set of all partitions $\{A_1,\ldots,A_r\}$, $r \in \mathbb{N}^+$ of Y with $\#A_i = 2$, $i = 1,\ldots,r$, is denoted by $\mathfrak{Par}(Y;2)$ For $x \in X \setminus S(\iota)$, the element $\{x,\iota(x)\} \in \mathfrak{p}(\iota)$ is a 2-element subset, since x is not a fixed point of ι, i. e., $x \neq \iota(x)$. Further, two subsets $\{x,\iota(x)\},\{y,\iota(y)\} \in \mathfrak{p}(\iota)$ are either equal or disjoint. – The inverse map of the map $\iota \mapsto \big(S(\iota),\mathfrak{p}(\iota)\big)$ is the map which assigns a $(S,\mathfrak{p})$ to the involution $\iota : X \to X$ defined by $\iota(x) := x$, if $x \in S$, and $\iota(x) := y$, if $x \notin S$ and $\{x,y\} \in \mathfrak{p}$.)

(b) Let X be a finite set. Then $\#X \equiv \#S(\iota) \pmod 2$, i. e., the number $\#X$ of elements in X and the number $\#S(\iota)$ of fixed points of ι have the same parity. In particular, every involution of a finite set with odd cardinality has a fixed point. (**Hint :** Let $\#\mathfrak{p}(\iota)| = k \in \mathbb{N}$. Since all elements of $\mathfrak{p}(\iota)$ are 2-element subsets, $\#(X \setminus S(\iota)) = \#\big(\biguplus_{A \in \mathfrak{p}(\iota)} A\big) = 2k$ and $\#X = \#S(\iota) + 2k$, i .e. $\#X \equiv \#S(\iota) \pmod 2$.)

(c) Let X be finite with even cardinality $\#X = 2n$, $n \in \mathbb{N}$. Then the number of fixed point free involutions on X is equal to the product $\prod_{k=1}^{n}(2k-1) = 1\cdot 3 \cdots (2n-1) = (2n)!/2^n n!$ of the first n odd natural numbers. (**Hint :** Let $\operatorname{Inv}_{\mathrm{f}}(X)$ denote the set of all fix-point free involutions on a set X. Let $\#X = 2n$ and let $s_n := \#\operatorname{Inv}_{\mathrm{f}}(X)$. Then prove the recursion $s_{n+1} = (2n+1)s_n$, $n \in \mathbb{N}$ and hence the equality $s_n = \prod_{k=1}^{n}(2k-1)$ by induction on n. For a proof of recursion, let $\#X = 2n+2$ and $a \in X$ be fixed. For $b \in X \setminus \{a\}$, let $\operatorname{Inv}_{\mathrm{f}}(X;a,b) := \{\iota \in \operatorname{Inv}_{\mathrm{f}}(X) \mid \iota(a) = b\}$. Then $\#\operatorname{Inv}_{\mathrm{f}}(X;a,b) = s_n$ for every $b \in X \setminus \{a\}$, since the restriction map $\operatorname{Inv}_{\mathrm{f}}(X;a,b) \xrightarrow{\approx} \operatorname{Inv}_{\mathrm{f}}(X \setminus \{a,b\})$, $\iota \mapsto \iota_{|X\setminus\{a,b\}}$ is bijective. Therefore $\#\operatorname{Inv}_{\mathrm{f}}(X) = \#\Big(\biguplus_{b \in X\setminus\{a\}} \operatorname{Inv}_{\mathrm{f}}(X;a,b)\Big) = (2n+1)s_n$. **Another Proof** (more direct) **:** For a set Y, let $\mathfrak{Par}_n(Y,2) = \{\mathfrak{p} = \{A_1,\ldots,A_n\} \in \mathfrak{Par}(Y) \mid \#A_i = 2, i = 1,\ldots,n\}$. By part (a) there is a bijection $\operatorname{Inv}_{\mathrm{f}}(X) \xrightarrow{\approx} \mathfrak{Par}_n(X;2)$ and every element $\mathfrak{p} = \{A_1,\ldots,A_n\}$ correspond to $n!$ decompositions $(A_1,\ldots,A_n)$ of X. Therefore, since the number of decompositions $(A_1,\ldots,A_n)$ of X into n subsets with $\#A_i = 2$ for all $i = 1,\ldots,n$, is (by Exercise 6.7) equal to $(2n)!/2^n$, we have $\#\operatorname{Inv}_{\mathrm{f}}(X) = \#\mathfrak{Par}_n(X;2) = (2n)!/2^n n! = 1\cdot 2\cdots(2n-1)\cdot 2n/2\cdot 4\cdots(2n) = 1\cdot 3\cdots(2n-1)$.)

(d) Let X be finite with $\#X = m \in \mathbb{N}$ arbitrary, then show that $\#\operatorname{Inv}(X) = \sum_{k=0}^{[m/2]} \binom{m}{2k} \dfrac{(2k)!}{2^k k!}$.

(**Hint :** Let $\#X = m \in \mathbb{N}$ be arbitrary. By part (a) $\#\operatorname{Inv}(X) = \#\{(S,\mathfrak{p}) \mid S \in \mathfrak{P}(X)$ and $\mathfrak{p} \in \mathfrak{Par}((X \setminus S);2)\}$. This is also equal to $\#\{(S,\iota) \mid S \in \mathfrak{P}(X)$ and $\iota \in \operatorname{Inv}_{\mathrm{f}}(X \setminus S)\}$. For fixed $S \in \mathfrak{P}(X)$ with $\#(X \setminus S) = 2k$ — we have just shown in the more direct proof of the part (c) that — the number of pairs (S,ι) is equal to $(2k)!/2^k k!$. Now, since $\#\mathfrak{P}_{2k}(X) = \binom{m}{2k}$, it follows that $\#\operatorname{Inv}(X) = \sum_{k=0}^{[m/2]} \binom{m}{2k} \dfrac{(2k)!}{2^k k!}$.)

^{R}**6.9**[3] (Latin Squares[4] and Finite Geometries) In 1782 Euler stated a problem : (Euler's Problem) This problem asks for *an arrangement of* 36 *officers of* 6 *ranks and from* 6 *regiments in a square formation of size* 6×6 *so that each vertical and each horizontal line of this formation contain one and only one officer of each rank and one and only one officer from each regiment.* Euler denoted regiments by the Latin letters a,b,c,d,e,f and the ranks by the Greek letters $\alpha,\beta,\gamma,\delta,\varepsilon,\zeta$. This was the origin of the term "*Graeco-Latin square*" (or, *Euler's Square*).

In modern terminology they are just called *Latin Squares* which are defined as : Let $n \in \mathbb{N}^*$. An $n \times n$ matrix $\mathfrak{A} = (a_{ij})_{1\le i,j\le n} \in \mathrm{M}_n(X)$ is called a Latin square with entries in a set X with $\#X = n$ if each row and each column of $\mathfrak{A}$ is a permutation of X.

[3] In this Exercise one can see that the history indicated that significant advances were made when one branch of mathematics was shown to be related to a different branch of mathematics.

[4] The great mathematician Leonhard Euler (1707-1783) introduced Latin squares in 1783 as a "nouveau espece de carres magiques", a new kind of magic squares. The name "*Latin square*" was inspired by mathematical papers by Leonhard Euler, who used Latin characters as symbols. Leonhard Euler was a Swiss mathematician who made enormous contributions to a wide range of mathematics and physics including analytic geometry, trigonometry, geometry, calculus and number theory.

(a) The binary operation table of a group G with $\#G = n$ is an $n \times n$ Latin square. In particular, the binary operation table of the group $(\mathbb{Z}_n, +_n)$ is an $n \times n$ Latin square.

Two Latin squares $\mathfrak{A} = (a_{ij})_{1 \leq i,j \leq n} \in \mathrm{M}_n(X)$ and $\mathfrak{B} = (b_{ij})_{1 \leq i,j \leq n} \in \mathrm{M}_n(Y)$ with entries in sets X and Y, respectively, with $\#X = n = \#Y$ are said to be orthogonal if every ordered pair $(x,y) \in X \times Y$ occurs as an entry in their *Hadamard product* $\mathfrak{A} \circ \mathfrak{B}$ or , equivalently, all pairs (a_{ij}, b_{ij}) are distinct.

(**Remarks :** Recall that the Hadamard product[5] (also known as the Schur product or the entry-wise product) of the two $m \times n$ matrices $\mathfrak{A} = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathrm{M}_{m,n}(X)$ and $\mathfrak{B} = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathrm{M}_{m,n}(Y)$ with entries in the sets X and Y, respectively, is the $m \times n$ matrix $\mathfrak{A} \circ \mathfrak{B} := ((a_{ij}, b_{ij}))_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathrm{M}_{m,n}(X \times Y)$ whose (i,j)-th entry is the ordered pair $(a_{ij}, b_{ij}) \in X \times Y$. — Euler defined orthogonal Latin squares and observed that the first step is to arrange Latin letters into a Latin square. In any case, if we label both the ranks and the regiments by $1, 2, \ldots, 6$, then Euler's problem reduces to the construction of a pair of orthogonal 6×6 Latin squares. Euler proved that :

(Euler's Theorem) *If $n \in \mathbb{N}^+$ and if $n \not\equiv 2$ (mod 4), then there exists a pair of orthogonal $n \times n$ Latin squares.*

Euler found no solution to his problem and then he conjectured that :

(Euler's Conjecture) *If $n \in \mathbb{N}^+$, $n > 2$ then there is no orthogonal pair $n \times n$ Latin squares if $n \equiv 2$* (mod 4).

The first case $n = 2$ is trivially impossible. In 1901, G. Tarry[6] proved by a systematic enumeration that Euler's conjecture holds for $n = 6$ and hence proved that there is no solution to the Euler's problems of 36 officers. E. T. Parker discovered an orthogonal pair of 10×10 Latin squares, there by disproving Euler's conjecture. However, it is not until 1960, through the combined efforts of R. C. Bose, S. S. Shrikhande and E. T. Parker[7] the remainder of Euler's conjecture is false. They proved that : *If $n \in \mathbb{N}^+$, $n > 6$ and if $n \equiv 2$* (mod 4)*, then there exists a pair of orthogonal $n \times n$ Latin squares.*)

There is an upper bound on the number of $n \times n$ Latin Squares that are pairwise orthogonal : *If $n \in \mathbb{N}^+$, $n > 2$ and if $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ are pairwise orthogonal $n \times n$ Latin Squares, then $r \leq n-1$.* If this upper bound is attained, then we say that there exists a complete orthogonal set of $n \times n$ Latin squares.

If $n = p^e$, $e \in \mathbb{N}^+$ is a power of a prime number p, then the following construction of orthogonal Latin squares uses the structure of a finite fields[8] $\mathbb{F}_{p^e}$:

(b) Let k be a finite field with $\#k = q$ and let $a \in k^\times$. Then the matrix $L_a := (ax + y)_{(x,y) \in k^2}$ is a $q \times q$ Latin square. Moreover, for $a, b \in k^\times$, $a \neq b$, the Latin squares L_a and L_b are orthogonal. In particular, for every prime power $p^e > 2$, L_a, $a \in k^\times$, is a complete orthogonal set of $p^e \times p^e$ Latin squares. (**Remark :** If we replace the finite field k by a finite ring $(\mathbb{Z}_n, +_n, \cdot_n)$, $n \in \mathbb{N}^+$, $n \geq 2$, then L_a is a Latin square if and only if a is a unit in the ring $\mathbb{Z}_n$, i. e., $a \in \mathbb{Z}_n^\times$. For which $a, b \in \mathbb{Z}_n^\times$, $a \neq b$, the Latin squares L_a and L_b are orthogonal?)

(c) (Geometries) The basic axioms that we use in the *Euclidean* (*plane*) *geometry*[9] of the real plane are : (i) Two distinct *points* determine a unique *line*. (ii) If L is a line and P is a point not on L, then there exists a unique line L' such that $P \in L'$ and L' is parallel to L, i. e., $L \cap L' = \emptyset$.

[5] It should not be confused with the more common matrix product. It is attributed to, and named after, either French mathematician Jacques Hadamard, or German mathematician Issai Schur.

[6] See : [G. Tarry, Le problẽme des 36 officers, *C. R. Assoc. Fran. Av. Sci.*, 1 (1900), 122-123, Vol. 2 (1901), 170-203.

[7] See : [R. C. Bose and S. S. Shrikhande, On the falsity of Euler's conjecture about the non-existence of two orthogonal latin squares of order 4t + 2, *Proc. Nat. Acad. Sci.*, 45 (1959), 734-737.] and [R. C. Bose, S. S. Shrikhande, and E. T. Parker, Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, 12 (1960), 189-203.]

[8] Evariste Galois (1811-1832) invented finite fields around 1830. Galois was a French mathematician who produced a method of determining when a general equation could be solved by radicals and is famous for his development of early group theory; In 1782 Euler constructed orthogonal $p^n \times p^n$ Latin squares in a (different) more complicated way.

[9] During 18-th and 19-th centuries non-Euclidean geometries were developed when alternatives to the condition (ii) were investigated. However, all these geometries contained infinitely many points and lines in them.

One can also make the following more general definition :

Definition (Affine plane) Let $\mathbb{A}$ be any set — called the set of *points* and let $\mathfrak{L} \subseteq \mathfrak{P}(\mathbb{A}) \setminus \{\emptyset\}$ — called the set of *lines*. An affine plane is a structure on the pair $(\mathbb{A}, \mathfrak{L})$ which satisfy the following three properties : (A1) Two distinct *points* determine a unique *line*. (A2) If L is a line and P is a point not on L, then there exists a unique line L' such that $P \in L'$ and L' is parallel to L, i. e., $L \cap L' = \emptyset$. (A3) There are at least 4 points in $\mathbb{A}$, no three of them are *collinear*, i. e., they do not lie on any line $L \in \mathfrak{L}$.

In the 17-th century, the co-ordinates were introduced by Fermat[10] and Descartes[11] with this Euclidean geometry became analytical geometry, there by points by coordinates and and lines are described algebraically by their equations and *slopes* : the lines $X = a$, $a \in \mathbb{R}$ are *vertical lines* (with infinite slopes); the lines $Y = mX + c$, $(m, c) \in \mathbb{R}^2$ are lines with finite slopes $m \in \mathbb{R}$ and two line are parallel if and only if they have the same slopes. The introduction of co-ordinates Euclidean geometry became the co-ordinate (or analytic) geometry. This also brought out the most important property used in Euclidean or analytic geometry, namely, the usual addition and the usual multiplication on the set of real numbers form a field and that one can solve quadratic equations with real coefficients.

We can therefore starting from an arbitrary field k (may be even finite) the following examples of affine planes (over k are useful :

Definition (Affine plane over a field) Let k be a field (may be even finite). Let $\mathbb{A}^2_k := k^2$ and let $\mathfrak{L}_k := \{\text{vertical lines} : L_a := X - a = 0 \mid a \in k\} \cup \{\text{lines with finite slopes} : L_{m,c} := Y - mX + c = 0 \mid (m, c) \in k^2\}$. One can easily check (using the field structure on k) that $(\mathbb{A}^2_k, \mathfrak{L}_k)$ has a structure of an affine plane (in the sense of above definition).

Now, if $k = \mathbb{F}_q$ is a finite field with q elements, then $\# \mathbb{A}^2_k = q^2$, each line $L \in \mathfrak{L}_k$ contains exactly q points, each point in $\mathbb{A}^2_k$ lies on exactly $q + 1$ lines and $\# \mathfrak{L}_k = q^2 + q$. These are specific examples of finite affine planes or finite geometries which have connection with the Latin squares, see the part (b) above.

What exactly goes wrong (which of geometric properties A1, A2, A3 in the definition of affine plane fail) if we try to construct an affine plane $\mathbb{A}^2_{\mathbb{Z}_4}$ or $\mathbb{A}^2_{\mathbb{Z}_6}$ using the finite rings $\mathbb{Z}_4$ or $\mathbb{Z}_6$ instead of a field?

We now introduce a construction that enlarges affine planes to what is called a *projective plane* :

Definition (Projective plane[12]) Let $\mathbb{P}$ be any set — called the set of *points* and let $\mathfrak{L} \subseteq \mathfrak{P}(\mathbb{P}) \setminus \{\emptyset\}$ — called the set of *lines*. A projective plane is a structure on the pair $(\mathbb{P}, \mathfrak{L})$ which satisfy the following three properties : (P1) Two distinct *points* determine a unique *line*. (P2) Any two lines $L, L' \in \mathfrak{L}$ intersect in a unique point $P \in \mathbb{P}$. (P3) There are at least 4 points in $\mathbb{P}$, no three of them are *collinear*, i. e., they do not lie on any line $L \in \mathfrak{L}$. We further say that $(\mathbb{P}, \mathfrak{L})$ is a projective plane of order n if $\# \mathbb{P} = n^2 + n + 1$.

The affine planes over a field are extended to projective planes as follows :

Definition (Projective plane over a field) Let k be a field (may be even finite). Start with an affine plane $\mathbb{A}^2_k$ and let $\mathbb{P}^2_k := \{(x, y, 1) \mid (x, y) \in \mathbb{A}^2_k \cup L_\infty$, where $L_\infty := \{(1, 0, 0)\} \cup \{(x, 1, 0) \mid x \in k\}$. Now think of points $(x, y, 1)$ as ordered triples $(x, y, z) \in k^3$, where $z = 1$ and rewrite the equations $L_a = X - a = 0$ and $L_{m,c} = Y - mX + c = 0$ of lines in $\mathbb{A}^2_k$ as : $L_a = X - aZ = 0$ and $L_{m,c} = Y - mX + cZ = 0$, where $Z = 1$. In addition to these lines add the new line L_∞ — called the *line at infinity* — which has the equation $Z = 0$ with the convention that we never have $x = y = z = 0$, i. e., $(0, 0, 0) \notin \mathbb{P}^2_k$. One can now easily check (using the field structure on k) that $(\mathbb{P}^2_k, \mathfrak{L}_k \cup \{L_\infty\})$ has a structure of a projective plane (in the sense of above definition). Moreover, if $k = \mathbb{F}_q$ is a finite field with q elements, then $\# \mathbb{P}^2_k = q^2 + q + 1$ elements, i. e., the finite projective plane $(\mathbb{P}^2_k, \mathfrak{L}_k \cup \{L_\infty\})$ has order q. Furthermore, each line $L \in \mathfrak{L}_k \cup \{L_\infty\}$ contains exactly

[10] Pierre de Fermat (1601-1665) was a French lawyer and government official most remembered for his work in number theory; in particular for *Fermat's Last Theorem*. He is also important in the foundations of the calculus.

[11] René Descartes (1596-1650) was a French philosopher whose work, La géométrie, includes his application of algebra to geometry from which we now have Cartesian geometry. His work had a great influence on both mathematicians and philosophers.

[12] Projective geometry has its origins in the early Italian Renaissance, particularly in the architectural drawings of Filippo Brunelleschi (1377 - 1446) and Leon Battista Alberti (1404 - 1472), who invented the method of perspective drawing. In the early 1800s, mathematicians were studying problems of perspective arising from artists painting pictures of three-dimensional scenes on two-dimensional canvases. To eye parallel lines seem to meet at the horizon, this suggests adjoining a new line called the "line at infinity" to the ordinary (affine) plane. With this this the concept of projective plane came into existence.

$q+1$ points, each point in $\mathbb{P}^2_k$ lie on exactly $q+1$ lines, there are exactly $\#\mathfrak{L}_k \cup \{L_\infty\} = q^2+q+1$ lines and any two points in $\mathbb{P}^2_k$ lie on only one line.

The difference between the affine and projective planes is that in projective planes there are no parallel lines. The smallest example of a finite projective plane[13] is a triangle– the projective plane of order 1. The smallest non-trivial example is of order 2, i. e., $\mathbb{P}^2_{\mathbb{F}_2}$ which has 7 points and 7 lines. It is possible to constructive projective planes without using finite fields. For example, it is known that there are four projective planes of order 9 and only one among them arises from the finite field with 9 elements.

— **Remarks :** One can generalize the definitions of affine and projective planes to higher dimensional affine and projective spaces using the *vector spaces* (over fields) of higher dimensions. Their study is then called *affine geometry* or *projective geometry*. Combinatorial designs[14] are related to finite projective geometries.

The following theorem is the reason for introducing the concept of (finite) projective planes :

Theorem (Bose, 1938)[15] *If $n \in \mathbb{N}^+$, $n \geq 3$, then there exists a projective plane of order n if and only if there exists a complete orthogonal set of $n \times n$ Latin squares.*

Since there does not exist even a pair of orthogonal 6×6 Latin squares, Bose's result implies the non-existence of a projective plane of order 6. Systematic hand enumeration is messy and is error prone. But mathematicians did find a better explanation in the following celebrated result of Bruck and Ryser :

Theorem (Bruck-Ryser, 1949)[16] *Suppose that $n \in \mathbb{N}^+$ with either $n \equiv 1 (\bmod 4)$, or $n \equiv 2 (\bmod 4)$. Then a necessary condition for the existence of a finite projective plane of order n is that n is a sum of squares,* i. e., *$n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$.*

An equivalent formulation of the Bruck-Ryser theorem is : *If a projective plane of order n exists and if $n \equiv 1,2 (\bmod 4)$, then the square-free part of n has no prime divisors of the form $3 (\bmod 4)$.*

We can deduce some simple corollaries : among the first few numbers of the form $1 (\bmod 4)$ are : $5, 9, 13, 17, 21, 25, 29, 33$, there are no projective planes of orders 21 and 33 ; among the first few numbers of the form $2 (\bmod 4)$ are : $6, 10, 14, 18, 22, 26, 30, 34$ there are no projective planes of orders $6, 14, 22$ and 30.

The crucial step involved in the proof of Bruck-Ryser Theorem is the use of *incidence matrix* $\mathfrak{A} \in \mathrm{M}_n(\{0,1\})$ of the projective plane of order n and its properties which are translated from the properties of the projective plane. Ryser showed that the incidence matrix $\mathfrak{A}$ is a normal matrix, i. e., $\mathfrak{A} \cdot {}^{\mathrm{tr}}\mathfrak{A} = {}^{\mathrm{tr}}\mathfrak{A} \cdot \mathfrak{A}$.

Since there exists a projective plane of order p, Bruck-Ryser Theorem implies the Fermat's two-square theorem: *If p is a prime number with $p \equiv 1 (\, mod\, 4)$, then p is a sum of two squares.* In fact, Bruck-Ryser Theorem implies that : *If p is a prime number with $p \equiv 1 (\, mod\, 4)$, then p^e is a sum of two squares for every $e \geq 2$.*

— **Remarks :** In 1988 C. Lam[17] was able to show that *there does not exist a projective plane of order* 10. He used a massive amount of calculation : 19,200 hours (approximately 800 days) on VAX-11/780 followed by 3,000 hours (approximately 3 months) on CRAY-1A. Thus, two and half years of actual computer running time (not counting the years of human thought and ingenuity involved in instructing the machines) solved the problem. It is unknown whether a projective plane of order 12 exists (since $12 \equiv 0 (\bmod 4)$, it is not covered by Bruck-Ryser theorem.)

[13] The notion of a finite projective planes did not appear until the end of 19-th century in the work of Gino Fano (1871-1952) an Italian mathematician. The Fano-plane is a projective plane of order 2, i. e., with 7 points. Another one of order 3, i. e., with 13 points was constructed by Tictac a theoretical physicists by adding to their word 4 points. The attractiveness of these objects is in their simplicity and their reliance on the language of geometry.

[14] Notion of designs was first studied by statisticians (R. A. Fisher and his followers) in the area called the design of experiments. This area play an important role in the modern theory of statistical analysis.

[15] See :[R. C. Bose, On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares, *Sankhyd*, 3 (1938) 323-338.]

[16] See : [R. H. Bruck and H. J. Ryser, The non-existence of certain finite projective planes, *Can. J. Math.*, 1 (1949) 88-93.]

[17] See : [C. W. H. Lam, L. H. Thiel, and S. Swiercz, The non-existence of finite projective planes of order 10, *Can. J. Math.*, XLI (1989), 1117-1123.]

(d) (Latin rectangles) Let $r,s \in \mathbb{N}^*$. A $r \times s$ matrix $\mathfrak{A} = (a_{ij}) \in \mathrm{M}_{r,s}(X)$ is called a Latin rectangle with entries in a set X if entries in each row and in each column of $\mathfrak{A}$ are distinct. Suppose that $\#X = n \geq \max\{r,s\}$, then we say that a Latin rectangle $\mathfrak{A} \in \mathrm{M}_{r,s}(X)$ is extendable to an $n \times n$ Latin square if it is possible to add $n-s$ columns and $n-r$ rows to $\mathfrak{A}$ such that it becomes an $n \times n$ Latin square. With this definition, prove that :

Theorem (Marshall Hall, 1945)[18] *Let $r,n \in \mathbb{N}^*$ with $r < n$. Then every $r \times n$ Latin rectangle $\mathfrak{A} = (a_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}} \in \mathrm{M}_{r,n}(X)$ with entries in a set X can be extended to an $n \times n$ Latin square.*

(**Proof :** Obviously $\#X \geq n$ and we may assume that $X = \{1,\ldots,n\}$ and that every row is a permutation of X. We use the Marriage Theorem T6.1 to the family $Y_j := \{i \in X \mid i \text{ does not appear in the } j\text{-th column}\}$, $j \in X$. Now, to verify that the Marriage condition is satisfied, it is easy to check that : (i) $\#Y_j = n-r$ for every $j \in X$. (ii) Every element of X appears exactly in $n-r$ subsets Y_j, $j \in X$. For this use the fact that every element of X appears exactly r times in the Latin rectangle. (iii) For every $m \in X$, any m sets Y_j, $j \in X$ together contain $m(n-r)$ elements and hence (by (ii)) at least m distinct elements. •)

R **6.10** **(a)** Let $a,b,m,k \in \mathbb{N}$ be such that $\binom{a}{k} \leq m < \binom{a+1}{k}$ and $\binom{b}{k} \leq m < \binom{b+1}{k}$. Show that $a = b$. (**Hint :** Suppose that $a < b$, i.e., $a+1 \leq b$. Then, since $\mathfrak{P}_k(\{1,\ldots,a+1\}) \subseteq \mathfrak{P}_k(\{1,\ldots,b\})$, we have $m < \binom{a+1}{k} \leq \binom{b}{k} \leq m$, a contradiction.)

(b) Let $k \in \mathbb{N}^+$ be a positive natural number and let $n \in \mathbb{N}$ be an arbitrary natural number. Show that there exist unique $a_1,\ldots,a_k \in \mathbb{N}$ such that $0 \leq a_1 < a_2 < \cdots < a_k$ and $n = \sum\limits_{j=1}^{k} \binom{a_j}{j}$. (**Hint :** The existence of $a_1,\ldots,a_k$ is proved by induction on k. If $k=1$, then $n = \binom{n}{1}$ is the required representation. Assume $k>1$ and choose $a_k \in \mathbb{N}$ with $\binom{a_k}{k} \leq n < \binom{a_k+1}{k}$. For the number $m := n - \binom{a_k}{k} \geq 0$ by induction hypothesis there exists a representation $m = \sum_{j=1}^{k-1} \binom{a_j}{j}$ with $0 \leq a_1 < a_2 < \cdots < a_{k-1}$. Now we need to show that $a_{k-1} < a_k$. Since $\binom{a_k+1}{k} = \binom{a_k}{k} + \binom{a_k}{k-1}$, we have $n = \sum_{j=1}^{k-1} \binom{a_j}{j} + \binom{a_k+1}{k} - \binom{a_k}{k-1} < \binom{a_k+1}{k}$; in particular, $\binom{a_{k-1}}{k-1} < \binom{a_k}{k-1}$ and hence $a_{k-1} < a_k$. Now we prove the uniqueness of $a_1,\ldots,a_k$. If $k=1$, this is trivial. Assume $k>1$ and suppose that $n = \sum_{j=1}^{k} \binom{a_j}{j} = \sum_{j=1}^{k} \binom{b_j}{j}$ with $0 \leq a_1 < a_2 < \cdots < a_k$ and $0 \leq b_1 < b_2 < \cdots < b_k$. It is enough to show that $\binom{a_k}{k} \leq n < \binom{a_k+1}{k}$ and $\binom{b_k}{k} \leq n < \binom{b_k+1}{k}$, for then, $a_k = b_k$ by part a) and by induction hypothesis to the two representations of $m := n - \binom{a_k}{k} = n - \binom{b_k}{k}$, we get $a_j = b_j$ for all $k = 1,\ldots,k-1$. Now, we show that $\binom{a_k}{k} \leq n < \binom{a_k+1}{k}$. If $a_k < k$, then $a_j = j-1$ for all $j = 1,\ldots,k$ and $\binom{a_k}{k} = \binom{k-1}{k} = 0 = n < \binom{a_k+1}{k} = \binom{k}{k} = 1$. Therefore suppose that $a_k \geq k$. Then $\binom{a_k+1}{k} = \sum_{i=0}^{k} \binom{a_k-i}{k-i}$ (by recursion formula [19]) and hence $\binom{a_k}{k} = \binom{a_k+1}{k} - \sum_{i=1}^{k} \binom{a_k-i}{k-i}$ and $n = \sum_{i=0}^{k} \binom{a_i}{i} = \sum_{j=1}^{k-1} \binom{a_{k-j}}{k-j} + \binom{a_k}{k} = \binom{a_k+1}{k} - \binom{a_k-k}{0} + \sum_{j=1}^{k-1} \left(\binom{a_{k-j}}{k-j} - \binom{a_k-j}{k-j} \right) = \binom{a_k+1}{k} - 1 - \sum_{j=1}^{k-1} \left(\binom{a_{k-j}}{k-j} - \binom{a_k-j}{k-j} \right)$. Now, since $a_k - 1 \geq a_{k-1}$ and by induction $a_k - j \geq a_{k-j}$ for every $1 \leq j \leq k-1$ and hence $\sum_{j=1}^{k-1} \left(\binom{a_{k-j}}{k-j} - \binom{a_k-j}{k-j} \right) \geq 0$. This proves that $n < \binom{a_k+1}{k}$, the other inequality $\binom{a_k}{k} \leq n$ is trivial.)

(c) For $k \in \mathbb{N}$, $k \geq 1$, show that the map $\mathbb{N}^k \to \mathbb{N}$ defined by

$$(m_1, m_2, \ldots, m_k) \mapsto \binom{m_1}{1} + \binom{m_1+m_2+1}{2} + \cdots + \binom{m_1+m_2+\cdots+m_k+k-1}{k}$$

is bijective. (**Hint :** Use part (b).)

Below one can see Lecture Notes.

[18] See : [Marshall Hall, An existence theorem for Latin squares, *Bull. Amer. Math. Soc.* Vol. 51 (1945), 387-293.]

[19] **Recursion formula for binomial coefficients:** $\binom{n+1}{k} = \binom{n}{k} + \binom{n-1}{k-1} + \cdots + \binom{n-k+1}{1} + \binom{n-k}{0}$. This follows from the equality $\binom{n+1}{m} = \binom{n}{m} + \binom{n}{m-1}$.