INFORMATION TO USERS

This material was produced from a microfilm copy of the original document. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the original submitted.

The following explanation of techniques is provided to help you understand markings or patterns which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting thru an image and duplicating adjacent pages to insure you complete continuity.

2. When an image on the film is obliterated with a large round black mark, it is an indication that the photographer suspected that the copy may have moved during exposure and thus cause a blurred image. You will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., was part of the material being photographed the photographer followed a definite method in "sectioning" the material. It is customary to begin photoing at the upper left hand corner of a large sheet and to continue photoing from left to right in equal sections with a small overlap. If necessary, sectioning is continued again — beginning below the first row and continuing on until complete.

4. The majority of users indicate that the textual content is of greatest value, however, a somewhat higher quality reproduction could be made from "photographs" if essential to the understanding of the dissertation. Silver prints of "photographs" may be ordered at additional charge by writing the Order Department, giving the catalog number, title, author and specific pages you wish reproduced.

5. PLEASE NOTE: Some pages may have indistinct print. Filmed as received.

Xerox University Microfilms
300 North Zeeb Road
Ann Arbor, Michigan 48106
CHANG, Kuang-I, 1948-
AN EXISTENCE THEORY FOR GROUP DIVISIBLE DESIGNS.
The Ohio State University, Ph.D., 1976
Mathematics

Xerox University Microfilms, Ann Arbor, Michigan 48106

© 1976
KUANG-I CHANG

ALL RIGHTS RESERVED
ACKNOWLEDGMENTS

I am thankful to Professor D. K. Ray-Chaudhuri for suggesting the problems of this thesis and also for many hours of stimulating discussions. I also express my sincere thanks to Professor Richard M. Wilson for very valuable help. My thanks are due to Professor J. C. Ferrar for his encouragement and my wife, Mary P. Chang, for her infinite patience. Acknowledgment is also due to the ONR research contract No. N00014-67-A-0232-0016 and NSF research grant No. MPS 75-08231.
VITA

October 2, 1948 ............... Born - Chianghsi, Republic of China

1969 ......................... B.S., Chung Yuan Christian College of Science and Engineering, Taiwan, Republic of China

1970-1974 ..................... Teaching Associate, Department of Mathematics, The Ohio State University, Columbus, Ohio

1971 .......................... M.S., The Ohio State University, Columbus, Ohio

1972-1973 ..................... Research Assistant, Department of Mathematics, The Ohio State University, Columbus, Ohio

1974-1976 ..................... Programmer B, Chemical Abstracts Service, Columbus, Ohio

1975-1976 ..................... Graduate Student, Department of Mathematics, The Ohio State University, Columbus, Ohio

FIELDS OF STUDY

Major Field: Mathematics


Studies in Algebra. Professor Joseph C. Ferrar

Studies in Analysis. Professor Bogdan M. Baishanski
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>11</td>
</tr>
<tr>
<td>VITA</td>
<td>111</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Chapter</td>
<td></td>
</tr>
<tr>
<td>I. PRELIMINARIES</td>
<td>12</td>
</tr>
<tr>
<td>Notations</td>
<td>12</td>
</tr>
<tr>
<td>Pairwise Balance Designs</td>
<td>13</td>
</tr>
<tr>
<td>Group Divisible Designs</td>
<td>23</td>
</tr>
<tr>
<td>Transversal Designs and Lattice Designs</td>
<td>34</td>
</tr>
<tr>
<td>II. GDD's AND (m,K,d)-PATTERNS</td>
<td>50</td>
</tr>
<tr>
<td>Necessary Conditions</td>
<td>50</td>
</tr>
<tr>
<td>Method of Differences</td>
<td>53</td>
</tr>
<tr>
<td>The Existence of GD(n,m,K)</td>
<td>56</td>
</tr>
<tr>
<td>(m,K,d)-Pattern</td>
<td>58</td>
</tr>
<tr>
<td>GDD's from (m,K,d)-Pattern</td>
<td>64</td>
</tr>
<tr>
<td>Existence of (m,K,d)-Pattern</td>
<td>69</td>
</tr>
<tr>
<td>Existence of Pseudo (m,K,d)-Pattern</td>
<td>75</td>
</tr>
<tr>
<td>Proof of the Existence Theorem for (m,K,d)-Pattern</td>
<td>83</td>
</tr>
<tr>
<td>$\beta(NG[m,K])$</td>
<td>88</td>
</tr>
<tr>
<td>III. EXISTENCE OF GD(n,m,K,\lambda)</td>
<td>93</td>
</tr>
<tr>
<td>A Construction</td>
<td>93</td>
</tr>
<tr>
<td>$\alpha(NG[m,k])$</td>
<td>100</td>
</tr>
<tr>
<td>$\alpha(NG[m,K])$</td>
<td>107</td>
</tr>
<tr>
<td>Existence of GD(n,m,K,\lambda)</td>
<td>109</td>
</tr>
<tr>
<td>Existence of GD(n,m,3)</td>
<td>114</td>
</tr>
<tr>
<td>IV. LATTICE DESIGNS</td>
<td>122</td>
</tr>
<tr>
<td>Preliminaries</td>
<td>122</td>
</tr>
<tr>
<td>A Direct Construction of LD's</td>
<td>130</td>
</tr>
</tbody>
</table>
### The Statement of the Existence Theorem for

| The Existence of LD(n,m,k) | 137 |
| The Existence of LD(n,m,K) | 142 |
| The Existence of LD(n,m,K,λ) | 144 |
| Special Cases | 148 |

### V. SUBDESIGNS, NONISOMORPHIC GROUP DIVISIBLE DESIGNS AND LATTICE DESIGNS

| Preliminaries | 155 |
| Sub-GDD's | 156 |
| Nonisomorphic GDD's | 164 |
| Nonisomorphic LD's | 169 |
| Nonisomorphic TD(k,m)'s | 173 |
| k = 3 | 179 |

### BIBLIOGRAPHY | 192
All definitions which we state briefly or take for granted here will be stated in detail in various chapters of the text. Let \( v \) and \( \lambda \) be given positive integers, and \( K \) a set of positive integers. A pairwise balanced design (PBD) on \( v \) treatments with block sizes from \( K \) and index of pairwise balance \( \lambda \) is an arrangement of the elements of a finite \( v \)-set \( V \) into sets, called blocks, such that the cardinality of each block is in \( K \) and the number of blocks containing any pair of elements of \( V \) is \( \lambda \). If \( K = \{k\} \), then it is known as a \((v,k,\lambda)\)-BIBD (balanced incomplete block design). The concept of BIBD was introduced in \([18, 25]\) by Kirkman and Steiner. They have arisen in the study of algebraic geometry. They occur also in the theory of the design of experiments in statistics.

One of the most central problems of modern combinatorial theory is the determination of those triples \((v,k,\lambda)\) for which there exists a \((v,k,\lambda)\)-BIBD. Much work has been done in this area, for example \([1, 3, 12, 13, 15, 16]\). It is well known that a necessary condition for the existence of a \((v,k,\lambda)\)-BIBD is that 
\[ r = \lambda(v - 1)/(k - 1) \] and 
\[ b = \lambda v(v - 1)/k(k - 1) \] are integers, or equivalently, \( \lambda(v - 1) \equiv 0 \pmod{(k - 1)} \) and \( \lambda v(v - 1) \equiv 0 \pmod{k(k - 1)} \). In \([20, 24]\), it was shown that the
necessary conditions are also sufficient for the existence of a
(v,3,l) -BIBD. In [12, 13, 15], it was shown that the same is
ture for k = 3, 4, 5 and any l, except the triple (15,5,2)
for which there is no (15,5,2) -BIBD as proved in [11]. In
[16], it has been shown that it is also true for k = 6 and
l > 1, k = 7 and l = 7, 42.

In fact, it was conjectured [10] that the necessary conditions
are also sufficient for the existence of a (v,k,l) -BIBD if k
and l are fixed and v is 'sufficiently large.' The conjecture
has been proved completely by R. M. Wilson [26, 27]. There, he
considered a more general problem, namely, the existence of a
(v,K,l) -PBD with block sizes from K, a set of positive integers
instead of a single block size k. If we define α(K) to be the
greatest common divisor (gcd) of the set \{k - 1 \mid k \in K\} and β(K)
to be gcd of the set \{k(k - 1) \mid k \in K\}, then the necessary
conditions for the existence of a (v,K,l) -PBD are
λ(v - 1) \equiv 0 (mod α(K)) and λv(v - 1) \equiv 0 (mod β(K)). He proved
that the necessary conditions above are sufficient for the
existence of a (v,K,l) -PBD if v is 'sufficiently large' with
fixed K and λ.

The following closure operation arises in his theory. For a
subset K of positive integers, let B[K] denote the set of
positive integers v for which there is a (v,K,l) -PBD. The
mapping K \rightarrow B[K] is a closure operation, i.e. (1) B[K] \supseteq K,
(2) if K_1 \supseteq K_2 , B[K_1] \supseteq B[K_2] , and (3) B[B[K]] = B[K], for
all subsets $K, K_1, K_2$ of positive integers. A subset $K$ of positive integers is said to be closed iff (if and only if) $K = B[K]$. R. M. Wilson has proved that a closed set $K$ is essentially determined by the parameters $\alpha(K)$ and $\beta(K)$. He proved that there exists a constant $t(K)$ such that if $k \in K$ and $k > t(K)$, then $k \in K$ iff $k$ is of the form $1 + a\alpha(K) + b\beta(K)$ where $a$ and $b$ are nonnegative integers such that $1 \leq 1 + a\alpha(K) \leq \beta(K)$ and $(1 + a\alpha(K))a(\alpha(K)) \equiv 0 \pmod{\beta(K)}$.

His proof also involved another very important combinatorial structure, called group divisible designs.

Let $v$ and $\lambda$ be positive integers, and $K$ and $M$ be subsets of positive integers. A group divisible design (GDD) on $v$ treatments with block sizes from $K$, group sizes from $M$, and index of pairwise balance $\lambda$ is a triple $(X, \mathcal{G}, \mathcal{A})$ where (i) $X$ is a set of $v$ elements, called points or treatments, (ii) $\mathcal{G}$ is a partition of $X$ such that $|G| \in M$ for every $G \in \mathcal{G}$, called groups, (iii) $\mathcal{A}$ is a family of subsets of $X$, called blocks, whose cardinalities are in $K$, (iv) every block intersects any group in at most one point, (v) every pair of points of $X$, not in the same group of $\mathcal{G}$, is contained in exactly $\lambda$ blocks of $\mathcal{A}$.

We can get a $(v, K \cup M, \lambda)$-PBD from a $(v, M, K, \lambda)$-GDD by taking each group as a block, $\lambda$ times. From a $(v, K, \lambda)$-PBD, we may obtain a $(v, [1], K, \lambda)$-PBD by regarding each point as a group of
size 1. We shall see some more intimate relationships between PBD's and GDD's in the text.

The combinatorial properties of GDD's (in a more general sense) was investigated in [2]. In this treatise, we will be concerned with those GDD's in which all groups have the same size, say \( m \). In this case, the number of points is \( nm \) for some positive integer \( n \). We shall denote the GDD by \( GD(n,m,K,X) \). For convenience, we shall write \( GD(n,m,K) \) instead of \( GD(n,m,K,1) \) and \( GD(n,m,k) \) instead of \( GD(n,m,(k),X) \).

Let \( NG[m,K,X] \) denote the set of positive integers \( n \) for which there exists a \( GD(n,m,K,X) \). (NG stands for the number of groups.) Particularly important and useful GDD's are those with \( k \) groups of size \( m \) and block size \( k \). Their existence is equivalent to the existence of \( k - 2 \) mutually orthogonal Latin squares of order \( m \) which in turn is equivalent to the existence of an \( (m^2,k,m,2) \) orthogonal array of strength 2.

The necessary conditions for the existence of a \( GD(n,m,K,X) \) are \( \lambda(n - 1)m \equiv 0 \pmod{\alpha(K)} \) and \( \lambda n(n - 1)m^2 \equiv 0 \pmod{\beta(K)} \).

One would naturally ask whether the necessary conditions are sufficient for the existence of a \( GD(n,m,K,X) \). Hanani [16] showed that the answer to the above question is affirmative for \( K = \{3\} \). One of our main results is

**Theorem 3.11'**. Given positive integers \( m \) and \( \lambda \), and a set \( K \) of positive integers, there exists a constant \( N = N(m,K) \)
such that if \( n > N \) is a positive integer and satisfies

\[
\lambda(n - 1)m \equiv 0 \pmod{\alpha(K)} \quad \text{and} \quad \lambda n(n - 1)m^2 \equiv 0 \pmod{\beta(K)},
\]

then a GD\((n,m,K,\lambda)\) exists.

In proving this theorem, we use the fact that the set \( \text{NG}[m,K,\lambda] \) is a closed set with respect to the closure operation \( B \). The main work is the determination of \( \beta(\text{NG}[m,K,\lambda]) \) and \( \alpha(\text{NG}[m,K,\lambda]) \). We will also give an independent proof for the existence of GD\((n,m,3)\). In the course of proving this theorem, we also derive many interesting results about GDD's.

Let \( m, n, \) and \( \lambda \) be given positive integers and let \( K \) be a set of positive integers. A lattice design (LD) on \( mn \) points with vertical group size \( n \), horizontal group size \( m \), block sizes from \( K \), and index of pairwise balance \( \lambda \) is a quadruple \( (X, \mathcal{V}, \mathcal{H}, \mathcal{A}) \) where (i) \( X \) is a finite set of \( nm \) elements, (ii) \( \mathcal{V} \) is a partition of \( X \) into \( m \) subsets of \( n \) elements each, called vertical groups, (iii) \( \mathcal{H} \) is a partition of \( X \) into \( n \) subsets of \( m \) elements each, called horizontal groups, (iv) each vertical group intersects a horizontal group in exactly one element, (v) \( \mathcal{A} \) is a family of subsets of \( X \) whose cardinalities are in \( K \), called blocks, (vi) each block intersects a horizontal or vertical group in at most one element, (vii) each pair of elements of \( X \) not belonging to any horizontal group or any vertical group is contained in exactly \( \lambda \) blocks of \( \mathcal{A} \).

LD's were first introduced in [5] (although with a different
terminology) and were used to construct GDD's. As we shall see in Chapters I and IV, the relationships among PBD's, GDD's, and LD's are very intimate. We shall use LD(n,m,K,λ) to denote an LD on nm points with vertical group size n, horizontal group size m, block sizes from K, and index of pairwise balance λ. Let \( \text{NHG}[m,K,λ] \) be the set of positive integers n for which an LD(n,m,K,λ) exists. Let \( \text{NVG}[n,K,λ] \) be the set of positive integers m for which an LD(n,m,K,λ) exists. (NHG and NVG stand for the number of horizontal and vertical groups, respectively.) We shall write LD(n,m,K) and LD(n,m,K,λ) instead of LD(n,m,K,1) and LD(n,m,K,1), respectively.

It is easily seen from the definition that an LD(n,m,K,λ) exists iff an LD(m,n,K,λ) exists (by exchanging the roles of vertical and horizontal groups). Thus, we shall restrict our attention to \( \text{NHG}[m,K,λ] \). All the results that we shall obtain in this treatise have corresponding ones for \( \text{NVG}[n,K,λ] \). There has never been any systematic investigation on the existence of LD(n,m,K,λ)'s. In this treatise, we shall give an 'asymptotically sufficient' condition for their existence.

As we shall see in Chapter I, the necessary conditions for the existence of LD(n,m,K,λ) are \( λ(n - 1)(m - 1) \equiv 0 \pmod{α(K)} \) and \( λn(n - 1)m(m - 1) \equiv 0 \pmod{β(K)} \). One of our main results is

Theorem 4.23'. Let K be a set of positive integers \( \geq 3 \).
There exists a constant $M_\lambda = M_\lambda (K)$ with the property that if $m > M_\lambda$ is a given positive integer and $\lambda$ is a given positive integer, then there exists a constant $C = C(m, K)$ such that an $LD(n, m, K, \lambda)$ exists for all positive integers $n > C$ satisfying the necessary conditions stated above.

In proving this theorem, we use the fact that the set $NHG[m, K, \lambda]$ is a closed set with respect to the closure operation $B$. The main work is the determination of $\beta(NHG[m, K, \lambda])$ and $\alpha(NHG[m, K, \lambda])$. In doing so, we have to construct a family of LD's by using the finite field and the difference method [1, 26, 27]. As consequences of Theorem 4.23, we have

**Theorem 4.29.** Let $m \geq 3$ and $\lambda$ be given positive integers. Then there exists a constant $\tilde{C}_3 = \tilde{C}_3 (m)$ such that an $LD(n, m, 3, \lambda)$ exists for all positive integers $n > \tilde{C}_3$ satisfying the necessary conditions stated above.

**Theorem 4.30.** Let $m \geq 4$ and $\lambda$ be given positive integers such that $m \not\in E_4$ where $E_4 = \{6, 10, 14, 15, 18, 22, 26, 30, 34, 38, 42, 46\}$. Then there exists a constant $\tilde{C}_4 = \tilde{C}_4 (m)$ such that an $LD(n, m, 4, \lambda)$ exists for all positive integers $n > \tilde{C}_4$ satisfying the necessary conditions stated above.

**Theorem 4.31.** Let $m \geq 5$ and $\lambda$ be given positive integers such that $m \not\in E_5$ where $E_5 = \{12, 14, 18, 21, 22, 24, 28, 33, 34, 38, 39, 42, 44, 48, 52, 54, 57, 58\}$. Then there exists a constant $\tilde{C}_5 = \tilde{C}_5 (m)$ such
that an LD\((n,m,5,\lambda)\) exists for all positive integers \(n > \tilde{c}_5\) satisfying the necessary conditions stated above.

**Theorem 4.32.** Let \(m \geq 6\) and \(\lambda\) be given positive integers such that \(m \not\in E_6\) where \(E_6 = \{14,20,26,35,38,44,50,62\}\). Then there exists a constant \(\tilde{c}_6 = \tilde{c}_6(m)\) such that an LD\((n,m,6,\lambda)\) exists for all positive integers \(n > \tilde{c}_6\) satisfying the necessary conditions stated above.

A GDD \((X',\mathcal{G}',\mathcal{A}')\) is a sub-GDD of a GDD \((X,\mathcal{G},\mathcal{A})\) iff

(i) \(X' \subseteq X\), (ii) \(\mathcal{A}' \subseteq \mathcal{A}\), (iii) every group of \(\mathcal{G}'\) is a subset of some unique group of \(\mathcal{G}\) and no two groups of \(\mathcal{G}'\) are contained in the same group of \(\mathcal{G}\). Let \(S\) and \(T\) be two sets of positive integers. We say that they **eventually coincide** iff there exists a constant \(C\) such that \([s \in S \mid s \geq C] = [t \in T \mid t \geq C]\).

For convenience, we shall write NG\([m,K]\) instead of NG\([m,K,1]\).

Let \(n_o\) and \(m_o\) be two given positive integers for which there is a GD\((n_o,m_o,K)\). Define \(S_K(n_o,m_o,m)\) to be the set of positive integers \(n\) for which there is a GD\((n,m,K)\) containing a GD\((n_o,m_o,K)\) as a sub-GDD. One of our main results is

**Theorem 5.7.** Let \(m, m_o\) be given positive integers such that \(m \geq m_o\). Let \(K\) be a set of positive integers. Let \(n_o\) be a positive integer such that a GD\((n_o,m_o,K)\) exists. If \(\frac{m_o}{(m,m_o)}, \alpha(K) = 1\), then NG\([m,K]\) and \(S_K(n_o,m_o,m)\) eventually
One of the very important problems in the theory of BIBD's is to determine the number of nonisomorphic BIBD's with a given parameter triple \((v,k,\lambda)\). In [27], it was shown that the number of nonisomorphic BIBD's with a given parameter triple \((v,k,\lambda)\) tends to infinity as \(v\) increases with given \(k\) and \(\lambda\) in a sequence such that the triple \((v,k,\lambda)\) satisfies the necessary conditions. One would naturally ask the same question for GD\((n,m,k,\lambda)\). Let \(n, m, k,\) and \(\lambda\) be given positive integers. Let \((X_1, \mathcal{G}_1, \mathcal{A}_1)\) and \((X_2, \mathcal{G}_2, \mathcal{A}_2)\) be two GD\((n,m,k,\lambda)\)'s. They are said to be isomorphic iff there exists a permutation \(\phi: X_1 \rightarrow X_2\) which maps groups onto groups and blocks onto blocks. Let \(N(n,m,k,\lambda)\) denote the number of nonisomorphic GD\((n,m,k,\lambda)\)'s. One of our main results is

**Theorem 5.11.** Let \(m \geq 2, k \geq 3,\) and \(\lambda\) be given positive integers. Then there exist constants \(s = s(m,k,\lambda) > 1\) and \(\tilde{N} = \tilde{N}(m,k,\lambda)\) such that \(N(n,m,k,\lambda) > s^n\) for all positive integers \(n > \tilde{N}\) for which a GD\((n,m,k,\lambda)\) exists. In particular, \(N(n,m,k,\lambda)\) tends to infinity as \(n\) increases with given \(m, k,\) and \(\lambda\) in a sequence such that the quadruple \((n,m,k,\lambda)\) satisfies the necessary conditions.

In this treatise, we also observe that \(N(n,m,3,1)\) tends to infinity as \(mn\) increases in a sequence such that the quadruple...
(n,m,3,1) satisfies the necessary conditions. Further, we shall observe that \( N(k,m,k,1) \) tends to infinity as \( m \) increases in a sequence such that the quadruple \((k,m,k,1)\) satisfies the necessary conditions.

Finally, noting the relationships among PBD's, GDD's and LD's, it would be unusual to choose to ignore the question on the number of nonisomorphic LD's with a given set of parameters. Let \( n, m, \) and \( \lambda \) be given positive integers and \( K \) be a set of positive integers. Let \( n, m, \) and \( \lambda \) be given positive integers and \( K \) be a set of positive integers. Let \( (X_1, \gamma_1, \lambda_1, \alpha_1) \) and \( (X_2, \gamma_2, \lambda_2, \alpha_2) \) be two LD\((n,m,K,\lambda)\)'s. They are said to be isomorphic iff there exists a permutation \( \phi: X_1 \rightarrow X_2 \) which maps horizontal groups to horizontal groups, vertical groups to vertical groups, and blocks to blocks. Let \( k \) be a positive integer. Let \( N_{\lambda}(n,m,k,\lambda) \) denote the number of nonisomorphic LD\((n,m,k,\lambda)\)'s. It was proven [8] that there exists a constant \( c(k) \) such that if \( m > c(k) \) is a given positive integer, then there are \( k - 2 \) mutually orthogonal Latin squares of order \( m \). Let \( \text{oa}(k) \) be the smallest such integer. One of our main results is

**Theorem 4.13.** Let \( k \geq 3 \) and \( \lambda \) be given positive integers. Let \( m > \text{oa}(k + 1) \) be a given positive integer. Then there exist constants \( t = t(m,k,\lambda) > 1 \) and \( \tilde{L} = \tilde{L}(m,k,\lambda) \) such that

\[
N_{\lambda}(n,m,k,\lambda) > t^{n^2}
\]

for all positive integers \( n \) for which an LD\((n,m,k,\lambda)\) exists. In particular, \( N_{\lambda}(n,m,k,\lambda) \) tends to infinity as \( n \) increases with fixed \( m, k, \) and \( \lambda \) in a sequence.
such that the quadruple \((n,m,k,\lambda)\) satisfies the necessary conditions.

This treatise is self-contained in the sense that no previous knowledge of the subject is assumed. Whenever we assume some results, we often refer the reader to the literature. The basic definitions and some of the basic results will be given in Chapter I.

Chapter II is devoted to constructing a family of GDD's so that we may have enough examples of GDD's to work with. There, we introduce a new combinatorial structure, \((m,K,d)\)-pattern.

Chapter III is devoted to proving the main theorem about the existence of GDD's. There, we use heavily some basic results in linear algebra.

In Chapter IV, we prove all our main results about the existence of LD's. There, we also construct a family of LD's with the aid of finite fields and difference methods as developed in [1, 26, 27]. Then we will apply one of the main results in [27] to our discussion in order to prove our main theorems.

Chapter V is devoted to a discussion of sub-GDD's and nonisomorphic GDD's and LD's.
§1.1 Notations. In this treatise, we will adopt the following terminology and conventions. \( \mathbb{Z} \) will denote the set of integers. \( \mathbb{N} \) will denote the set of positive integers, while \( \mathbb{N}_0 \) will denote the set of nonnegative integers. \( |S| \) will denote the cardinality of the set \( S \). If \( |S| = n \), we will call \( S \) an \( n \)-set. But, if \( |S| = 1 \), we will call \( S \) a singleton set. For \( n \in \mathbb{N} \), \( \mathbb{I}_n \) will denote the set \( \{1, 2, \ldots, n\} \) and \( \mathbb{Z}_n \) will denote the set of residue classes of \( \mathbb{Z} \) modulo \( n \). If \( a \) and \( b \) are in \( \mathbb{Z} \), \( (a, b) \) will denote the greatest common divisor (g.c.d.) of \( a \) and \( b \). For a subset \( S \subset \mathbb{Z} \), \( \text{gcd}(S) \) is defined to be the unique nonnegative generator of the ideal in \( \mathbb{Z} \) generated by \( S \). Let \( X \) and \( Y \) be two sets. \( X \times Y \) denotes the set \( \{(x, y) \mid x \in X, y \in Y\} \). Let \( q \) be a prime power. \( \text{GF}(q) \) denotes the finite field of \( q \) elements.

By a list, we mean a collection of objects in which each object appears with a certain nonnegative multiplicity. More formally, a list of elements of a finite set \( S \) may be regarded as a mapping \( f: S \to \mathbb{N}_0 \) where \( f(x) \) is called the multiplicity of \( x \) in the list \( f \). If \( f \) and \( g \) are two lists of elements of a finite set \( X \), we define \( f + g: X \to \mathbb{N}_0 \) by setting
\((f + g)(x) = f(x) + g(x)\) for every \(x \in X\), and we define, for any \(c \in \mathbb{N}_0\), \(cf: X \to \mathbb{N}_0\) as \((cf)(x) = c(f(x))\). Let \(f\) be a list on \(X\). If \(f(x) > 0\), we say that \(x\) occurs in the list \(f\) and \(f(x)\) is its multiplicity, or \(x\) occurs \(f(x)\) times in the list \(f\). However, we shall be informal and take list as a primitive concept.

Let \(f\) be a list on \(X\). We will sometimes describe a list by writing the element \(x\), within parentheses, \(f(x)\) times, for each \(x\) with \(f(x) > 0\). Of course, the order is not important. Sometimes, a list will be denoted by writing down the distinct elements occurring in the list, each enclosed in braces and preceded by its multiplicity, within parentheses. For example, the list \((x_1, x_2, x_3, y, x, x)\) of the set \(X = \{x_1, x_2, x_3, y, x, x\}\) will be represented as \((1 \cdot \{x_1\}, 2 \cdot \{x_2\}, 4 \cdot \{x\})\). In general, a list on a finite set \(X\) will be denoted by \((a_i \mid i \in I)\) where \(a_i \in X\) for every \(i \in I\) and \(I\) is some indexing set.

To avoid confusion, a set of subsets of a set will be called a class while a list of subsets of a set will be called a family. \(\emptyset\) will denote the empty class of subsets of a set. \(\mathcal{P}(X)\) will denote the class of all subsets of \(X\).

\[ \text{§1.2 Pairwise Balance Designs.}\] In 1852, Steiner [25] raised the following question:

For what positive integer \(v\) is it possible to form triples, out of \(v\) given elements, in such a way that
every pair of those \( v \) given elements appears in exactly one triple?

One can also ask the same question with the word 'triples' replaced by 'quadruples,' 'quintuple,' etc. More generally, one can ask the same question with the phrase 'exactly one' replaced by 'exactly \( \lambda \)' where \( \lambda \in \mathbb{N} \). This leads us to the following definition:

**Definition.** Let \( v, k, \) and \( \lambda \in \mathbb{N} \). A \((v,k,\lambda) - \text{BIBD}\) (balanced incomplete block design) is a pair \((X, \mathcal{B})\) where

(i) \( X \) is a finite set of \( v \) elements,
(ii) \( \mathcal{B} \) is a family of \( k \)-subsets of \( X \), say \( \mathcal{B} = \{ B_i \mid i \in I \} \),
(iii) for every 2-set \( \{ x, y \} \subset X \), the number of indices \( i \in I \) such that \( \{ x, y \} \subseteq B_i \) is exactly \( \lambda \).

For \( k = 3 \) and \( \lambda = 1 \), a \((v,3,1) - \text{BIBD}\) is known as a Steiner triple system. For \( v = 0 \), \((\emptyset, \emptyset)\) is \((0,k,\lambda) - \text{BIBD}\) for any \( k, \lambda \in \mathbb{N} \). For \( v = 1 \), \((\{x\}, \emptyset)\) is \((1,k,\lambda) - \text{BIBD}\) for any \( k, \lambda \in \mathbb{N} \). For \( v = k \), \((X, \mathcal{B})\) is a \((k,k,\lambda) - \text{BIBD}\) where \( X \) is a \( k \)-set and \( \mathcal{B} = (\lambda \cdot \{X\}) \). For \( k = 2 \), the construction of \((v,2,\lambda) - \text{BIBD}\) is trivial; we obtain such a \( \text{BIBD} \) by taking all 2-sets \( \{x, y\} \subset X \), each \( \lambda \) times. The elements of \( X \) will be called points or treatments and the elements of \( \mathcal{B} \) will be called blocks or lines. More generally, the pair \((X, \mathcal{B})\) will be called a design where \( X \) is a finite set and \( \mathcal{B} \) is a family of subsets of \( X \). A well-known theorem states that
Proposition 1.1. Let $v$, $k$, and $\lambda \in \mathbb{N}$. The necessary conditions for the existence of a $(v,k,\lambda)$ - BIBD are

$$\lambda(v - 1) \equiv 0 \pmod{(k - 1)}, \text{ and}$$

$$\lambda v(v - 1) \equiv 0 \pmod{k(k - 1)}$$

(1.1) (1.2)

Proof: This can be easily verified by counting the triples $(x,y,B)$ where $x,y \in X$, $x \neq y$, and $B$ is a block such that $(x,y) \in B$, and the triples $(x_0,y,B)$ where $x_0 \in X$ is any fixed elements, $y \in X$, $y \neq x$, and $B$ is a block such that $(x_0,y) \in B$. For details, see [26].

The number $r = \lambda(v - 1)/(k - 1)$ is called the replication number of this BIBD and is actually the number of indices $i$ such that $i \in I$ and $A_i$ contains a fixed point $x_0$ of $X$. This number does not depend on the particular point $x_0$. The number $b = \lambda v(v - 1)/k(k - 1)$ is actually the cardinality of the indexing set $I$. The number $k$ is called the block size of this BIBD.

BIBD's have application in the theory of statistical design of experiments. Naturally, one would like to find the triples $(v,k,\lambda)$ for which a $(v,k,\lambda)$ - BIBD exists. In view of Proposition 1.1, it is the same as to ask whether or not (1.1) and (1.2) are sufficient for the existence of a $(v,k,\lambda)$ - BIBD. For $k = 3$ and $\lambda = 1$, Reiss [24] and Moore [20] have shown that (1.1) and (1.2) are sufficient for the existence of a $(v,3,1)$ - BIBD. Recently, it has been shown [12, 13] that (1.1) and (1.2) are sufficient for
the existence of a \((v, k, \lambda) - \text{BIBD}\) for \(k = 3\) and \(4\). For \(k = 5\), it was shown [11] that a \((15, 5, 2) - \text{BIBD}\) did not exist. But Hanani [15, 16] showed that (1.1) and (1.2) were sufficient for the existence of a \((v, 5, \lambda) - \text{BIBD}\) where \((v, \lambda) \neq (15, 2)\).

M. Hall and W. S. Cornor [11] have shown that a \((21, 6, 2) - \text{BIBD}\) does not exist. However, Hanani [16] has shown that (1.1) and (1.2) are sufficient for the existence of a \((v, 6, \lambda) - \text{BIBD}\) where \(\lambda > 1\) and \((v, 6, \lambda) \neq (21, 6, 2)\). Also in [16], it was proven that (1.1) and (1.2) are sufficient for the existence of a \((v, 7, \lambda) - \text{BIBD}\) where \(\lambda = 7, \frac{42}{7}\). Some authors, for example [4, 12, 15] found it convenient to introduce more than one block size in proving their results. This leads us to the following definition:

**Definition.** Let \(v, \lambda, k \in \mathbb{N}\), and \(K \subseteq \mathbb{N}\). A \((v, k, \lambda) - \text{PBD}\) (pairwise balanced design on \(v\) treatments with block sizes from \(K\) and index of pairwise balance \(\lambda\)) is a pair \((X, \mathcal{A})\) where

1. \(X\) is a finite set of \(v\) elements,
2. \(\mathcal{A}\) is a family of subsets of \(X\), say \(\mathcal{A} = (B_i | i \in I)\) for some indexing set \(I\), such that \(|B_i| \in K\) for \(i \in I\),
3. for any 2-set \([x, y] \subseteq X\), the number of indices \(i \in I\) such that \([x, y] \subseteq B_i\) is precisely \(\lambda\).

Note that when \(K = \{k\}\), a \((v, (k), \lambda) - \text{PBD}\) is in fact a \((v, k, \lambda) - \text{BIBD}\). However, there has never been any systematic investigation of their existence until R. M. Wilson [26, 27] gave
an 'asymptotically sufficient' condition for their existence. For the rest of this section, we shall list some of his results which will be used in this treatise, and shall adopt his terminology and notations.

Given $K \subseteq \mathbb{N}$ and $\lambda \in \mathbb{N}$, let $B[K;\lambda] = \{v \in \mathbb{N} \mid a(v,K,\lambda) - \text{PBD exists}\}$. If $K = \{k\}$, write $B[k;\lambda]$ instead of $B[\{k\};\lambda]$. If $\lambda = 1$, write $B[K]$ for $B[K;1]$. Although $(\emptyset,\emptyset)$ is a $(0,\emptyset,\lambda) - \text{PBD}$, we exclude 0 from the set $B[K;\lambda]$. However, $((x),\emptyset)$ is a $(1,\emptyset,\lambda) - \text{PBD}$ and, for any $k \in K$, $(I_k, \lambda \cdot I_k)$ is a $(k,\emptyset,\lambda) - \text{PBD}$. Hence $1 \in B[K;\lambda]$ and $K \subseteq B[K;\lambda]$. Recall the definition of $\gcd(S)$ of a set $S$ in §1.1. One can observe very easily the following proposition.

**Proposition 1.2.** Let $K,L \subseteq \mathbb{N}$.

(i) $\gcd(K) = 0$ iff $K = \emptyset$ or $K = \{0\}$,

(ii) if $L \subseteq K$, then $\gcd(K) \mid \gcd(L)$,

(iii) there is a finite set $K_o \subseteq K$ such that $\gcd(K_o) = \gcd(K)$.

**Proof:** (i) and (ii) are trivial. For (iii), we note that since $\gcd(K)$ is an element of the ideal of $\mathbb{Z}$ generated by $K$ we may write $\gcd(K) = a_1 k_1 + a_2 k_2 + \ldots + a_n k_n$ for some $a_i \in \mathbb{Z}$, $k_i \in K$. Put $K_o = \{k_1, k_2, \ldots, k_n\}$. It is clear to see that $\gcd(K_o) = \gcd(K)$.

Let $X$ be a set and $\mathcal{A} = \{B_i \mid i \in I\}$ a family of subsets of $X$. We define, on the design $(X,\mathcal{A})$, its incidence relation $\rho$, 
for $x \in X$ and $i \in I$, by

$$\rho(x,B_i) = \begin{cases} 
1 & \text{if } x \in B_i, \\
0 & \text{if } x \notin B_i.
\end{cases}$$

Given $K \subseteq \mathbb{N}$, we define $\beta(K) = \gcd\{k(k - 1) \mid k \in K\}$. Then we have the following proposition.

**Proposition 1.3.** If $v \in B[K;\lambda]$, then $\lambda v(v - 1) \equiv 0 \pmod{\beta(K)}$.

**Proof:** Let $(X,\mathcal{I})$ be a $(v,K,\lambda)$-PBD. For every 2-set $(x,y) \subseteq X$, we have $\lambda = \sum_{i \in I} \rho(x,B_i) \rho(y,B_i)$. Thus,

$$\lambda v(v - 1) = \sum_{i \in I} \sum_{x,y \in X, x \neq y} \rho(x,B_i) \rho(y,B_i).$$

But for each $i \in I$, the inner sum is $|B_i|(|B_i| - 1) \equiv 0 \pmod{\beta(K)}$. Hence we have $\lambda v(v - 1) \equiv 0 \pmod{\beta(K)}$.

Given $K \subseteq \mathbb{N}$, we define $\alpha(K) = \gcd\{k - 1 \mid k \in K\}$. As before, we get the following proposition.

**Proposition 1.4.** If $v \in B[K;\lambda]$, then $\lambda(v - 1) \equiv 0 \pmod{\alpha(K)}$.

**Proof:** Using the same notations as above we have again

$$\lambda = \sum_{i \in I} \rho(x_o,B_i) \rho(y,B_i)$$

for any fixed $x_o \in X$ and for any $y \in X$, $y \neq x_o$. Thus, we have
\[ \lambda(v - 1) = \sum_{i \in I} \rho(x, B_i) \sum_{y \in X, y \neq x_0} \rho(y, B_i). \]

But if \( \rho(x_0, B_1) \neq 0 \), then \( \sum_{y \in X, y \neq x_0} \rho(y, B_i) = |B_i| - 1 = 0 \) (mod \( \alpha(K) \)). Hence, \( \lambda(v - 1) \equiv 0 \) (mod \( \alpha(K) \)).

Hence, the following are necessary conditions for the existence of a \((v, K, \lambda) - \text{PBD}\)

\[ \lambda(v - 1) \equiv 0 \pmod{\alpha(K)}, \text{ and} \quad (1.3) \]

\[ \lambda \nu(v - 1) \equiv 0 \pmod{\beta(K)} \quad (1.4) \]

One of the main results in [27] is as follows:

**Theorem 1.5.** Given \( K \subseteq \mathbb{N} \) and \( \lambda \in \mathbb{N} \). \( B[K; \lambda] \) contains all sufficiently large integers \( v \in \mathbb{N} \) satisfying (1.3) and (1.4).

To prove Theorem 1.5, R. M. Wilson has used the concept of closed sets.

**Definition.** By a closure operation on a set \( S \), we mean a mapping \( \varphi: \mathcal{P}(S) \to \mathcal{P}(S) \) such that

(i) \( S \subseteq \varphi(S) \),

(ii) \( \varphi(\varphi(S)) = \varphi(S) \),

(iii) for all \( A \subseteq B \subseteq S \), \( \varphi(A) \subseteq \varphi(B) \).
A subset \( A \subseteq S \) is said to be \textit{closed} with respect to a given closure operation \( \varphi \) iff \( A \) is equal to its \textit{closure} \( \varphi(A) \).

Evidently, a subset \( A \subseteq S \) is closed iff \( \varphi(A) \subseteq A \). We observe two elementary but useful facts concerning PBD's.

\textbf{Proposition 1.6.} If \( \lambda = \lambda_1 + \lambda_2 + \ldots + \lambda_n \) for some \( \lambda_i \in \mathbb{N} \) and \( a_i \in \mathbb{N}_0 \), and if \( K_1 \subseteq K \subseteq \mathbb{N} \), then

\[ \bigcap_{i=1}^{n} B(K_i; \lambda_i) \subseteq B(K; \lambda) \]

\textbf{Proof:} Let \( v \in \bigcap_{i=1}^{n} B(K_i; \lambda_i) \) and \( X \) be a \( v \)-set. Let \( (X, A) \) be a \( (v, K_i; \lambda_i) \) - PBD for every \( i \in I_n \). Set

\[ A = a_1 A_1 + \ldots + a_1 A_n. \]

Then \( (X, A) \) is a \( (v, K, \lambda) \) - PBD.

\textbf{Corollary 1.7.} If \( \lambda_0 | \lambda \), then \( B(K; \lambda_0) \subseteq B(K; \lambda) \).

\textbf{Proposition 1.8.} \( B[B(K; \lambda_1); \lambda_2] \subseteq B[K; \lambda_1 \lambda_2] \).

\textbf{Proof:} Let \( v \in B[B(K; \lambda_1); \lambda_2] \) and \( X \) be a \( v \)-set. Then there is a \( (v, B(K; \lambda_1); \lambda_2) \) - PBD, say \( (X, A) \) where \( A = (B_i | i \in I) \).

Now each \( |B_i| \subseteq B(K; \lambda_1) \) and hence, a \( (|B_i|, K, \lambda_1) \) - PBD exists, say \( (B_i, A_i) \) where \( A_i = (B_{ij} | j \in J_i) \) for some indexing set \( J_i \).

Let \( C = \Sigma_{i \in I} A_i = (B_{ij} | i \in I, j \in J_i) \). Then \( (X, C) \) is a \( (v, K, \lambda_1 \lambda_2) \) - PBD. Indeed, any 2-set \( \{x, y\} \subseteq X \) may occur in a block \( B_{ij} \) iff \( \{x, y\} \subseteq B_i \). There are \( \lambda_2 \) indices \( i \in I \) such that \( \{x, y\} \subseteq B_i \), and for each such \( i \) there are \( \lambda_1 \) indices.
Proposition 1.9. The mapping $B: \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ such that $B: K \to B[K]$ is a closure operation.

Proof: In view of Proposition 1.8, the result is easily seen to be true.

From now on, by closed set we mean a closed set with respect to the closure operation $B$. One can observe very easily that the sets $B[K;\lambda]$ are closed. The proof of Theorem 1.5 is actually to seek the description of a closed set, namely $B[K;\lambda]$, in terms of $\alpha(K)$ and $\beta(K)$. The proof of Theorem 1.5 involves the construction of a class of PBD's with the aid of finite fields and Theorem 1.11 (stated below), and another combinatorial structure, namely group divisible design. The following two theorems of [26, 27, 28] will be used in this treatise. So we state them without proof (for proof, see [26, 27, 28]).

Theorem 1.10. Let $K \subseteq \mathbb{N}$ be a closed set (i.e. $K = B[K]$).
Then $K$ contains all sufficiently large integers $v \in \mathbb{N}$ satisfying

\begin{align*}
    v &\equiv 1 \pmod{\alpha(K)}, \quad \text{and} \quad (1.5) \\
    v(v - 1) &\equiv 0 \pmod{\beta(K)} \quad (1.6)
\end{align*}

(and, in particular, all large $v \equiv 1 \pmod{\beta(K)}$.)

This theorem is a special case of Theorem 1.5 when we
specify \( \lambda = 1 \) in Theorem 1.5.

Let \( q \in \mathbb{N} \) be a prime power. Assume \( q \equiv 1 \pmod{e} \). Let \( \omega \) be a primitive element of \( \text{GF}(q) \). We define the cosets modulo the \( e \)-th powers, \( H^e_0, H^e_1, \ldots, H^e_{e-1} \), by

\[
H^e_m = \{ \omega^t \mid t \equiv m \pmod{e} \}, \quad m = 0, 1, 2, \ldots, e - 1.
\]

\( \mathcal{H}^e \) will denote the class of cosets \( \{H^e_0, H^e_1, \ldots, H^e_{e-1}\} \). Let \( r \geq 2 \) be an integer and let \( P(r) = \{(i,j) \mid 1 \leq i < j \leq r\} \).

Define a choice to be any map \( C: P(r) \to \mathcal{H}^e \), assigning to each \( (i,j) \in P(r) \) a coset \( C(i,j) \) modulo the \( e \)-th power in \( \text{GF}(q) \). An \( r \)-tuple \( (a_1, a_2, \ldots, a_r) \) of elements of \( \text{GF}(q) \) is said to be consistent with the choice \( C \) iff \( a_j - a_i \in C(i,j) \) for all \( 1 \leq i < j \leq r \).

**Theorem 1.11.** If \( q \equiv 1 \pmod{e} \) is a prime power and \( q > e^r(r-1) \), then, for any choice \( C: P(r) \to \mathcal{H}^e \), there exists an \( r \)-tuple \( (a_1, a_2, \ldots, a_r) \) of elements of \( \text{GF}(q) \) consistent with \( C \).

We note here that, if \((X, \mathcal{A})\) is a \((v,K,1)\) - PBD, then no block of size greater than one may occur more than once in \( \mathcal{A} \). In fact, if \( 1 \notin K \), then all blocks occur exactly once in \( \mathcal{A} \). Hence we may assume that \( \mathcal{A} \) is a class of subsets when \( \lambda = 1 \).

Furthermore, if \( 1 \in K \), \( \mathcal{A} \) may contain blocks of size one. But this does not affect anything. Hence \( B[K] = B[K \cup \{1\}] \).
§ 1.3 Group Divisible Designs. Let $X$ be a $v$-set. A class of nonempty subsets $C \subseteq P(X)$ is called a parallel class on $X$ iff $C$ is a partition of $X$. Let $K \subseteq \mathbb{N}$ and $(X, \mathcal{C})$ be a $(v,K,1)$-PBD. Let $x_0 \in X$ be any fixed element. Let $B_1, B_2, \ldots, B_r$ be the blocks which contain $x_0$ and $|B_i| > 1$ for every $i = 1, 2, \ldots, r$. Let $X' = X - \{x_0\}$, $B'_1 = B_i - \{x_0\}$ for $i = 1, 2, \ldots, r$, and $\mathcal{C}' = \{B \in \mathcal{C} \mid x_0 \notin B\}$. Let $y \in X'$. Then there is a unique $i \in I_r$ such that $(x_0, y) \subseteq B'_i$. Hence $C = \{B'_i \mid i \in I_r\}$ is a partition of $X'$, i.e., $C$ is a parallel class on $X'$. For any 2-set $\{x, y\} \subseteq X'$ such that $\{x, y\}$ is not contained completely in any $B'_i$, $i \in I_r$, there is a unique block $B \in \mathcal{C}'$ such that $\{x, y\} \subseteq B$. This leads us to the following definition of a very important combinatorial structure.

**Definition.** Let $v \in \mathbb{N}$, $\lambda \in \mathbb{N}$, $M \subseteq \mathbb{N}$, and $K \subseteq \mathbb{N}$. A $(v,M,K,\lambda)$-GDD (a group divisible design on $v$ treatments with group sizes from $M$, block sizes from $K$, and index of pairwise balance $\lambda$) is a triple $(X, \mathcal{L}, \mathcal{C})$ where

(i) $X$ is a finite set of $v$ elements,

(ii) $\mathcal{L}$ is a parallel class on $X$ and $|G| \in M$ for every $G \in \mathcal{L}$,

(iii) $\mathcal{C}$ is a family of subsets of $X$, say $\mathcal{C} = (B_i \mid i \in I)$, and $|B_i| \in K$ for every $i \in I$,

(iv) $|G \cap B_i| \leq 1$ for every $G \in \mathcal{L}$ and every $i \in I$,

(v) for any 2-set $\{x, y\} \subseteq X$ such that $\{x, y\}$ is not
contained completely in any \( \mathcal{G} \in \mathcal{J} \), the number of indices \( i \in I \) such that \((x, y) \in B_i\) is precisely \( \lambda \).

The elements of \( X \) will be called **points** or **treatments**, the elements of \( \mathcal{J} \) will be called **groups**, and the entries of \( \mathcal{A} \) will be called **blocks** or **lines**. The combinatorial properties of GDD's (in a more general sense, although with constant block size and group size) were investigated in [2]. As we observed at the beginning of this section, group divisible designs arise from PBD's in a very natural way. Here, we will present another way (although simple-minded) to get a group divisible design from a PBD. Let \((X, \mathcal{A})\) be a \((v, K, \lambda)\)-PBD. Let \( \tilde{X} = \{ \{ x \} | x \in X \} \). Then it is clear to see that \((X, \tilde{X}, \mathcal{A})\) is a GDD. Let \((X, \mathcal{J}, \mathcal{A})\) be a GDD. The list of integers \( (m_G | G \in \mathcal{J}) \) will be called the **group type** of this GDD where \( m_G = |G| \) for every \( G \in \mathcal{J} \). Define

\[
G_K[M, \lambda] = \{ v | v \in \mathbb{N}, a (v, M, K, \lambda) \text{-GDD exists} \}.
\]

(This notation is a slight generalization of that introduced in [26] by R. M. Wilson where \( \lambda = 1 \).) We have already observed how to get GDD from PBD. Now let us observe how to get PBD from GDD. It is easy to see that \( G_K[M, \lambda] \subseteq B[K \cup M, \lambda] \). Indeed, if we take each group \( \lambda \) times and combine them with the blocks of the GDD, we get a PBD with block sizes from \( K \cup M \) and index of pairwise balance \( \lambda \). We observe the following lemmas.

**Lemma 1.12.** Let \( K, M \subseteq \mathbb{N} \) and \( M' = \{ m + 1 | m \in M \} \). If \( v \in G_K[M, \lambda] \), then \( v + 1 \in B[K \cup M', \lambda] \).
Proof: Let \((X, \mathcal{A}, \mathcal{D})\) be a \((v, M, K, \lambda)\)-GDD. Take an element which is not in \(X\). Let us denote it by \(\omega\). Let \(X' = X \cup \{\omega\}\) and \(G' = G \cup \{\omega\}\) for every \(G \in \mathcal{D}\). Take each \(G'\) for \(G \in \mathcal{D}\), \(\lambda\) times, and combine them with all the blocks of \(\mathcal{A}\). Denote the resulting family by \(\mathcal{A}'\). Then \((X', \mathcal{A}')\) is a \((v+1, M' \cup K, \lambda)\)-PBD. Indeed, for any \(x \in X'\), \(x\) is in a unique group, say \(G\). Then \([x, \omega]\) is in exactly \(\lambda\) blocks of \(\mathcal{A}'\), namely \(G\) (\(\lambda\) times). Let \([x, y]\) \(\subseteq X\) be any 2-set. If \([x, y]\) \(\subseteq G\) for some \(G \in \mathcal{D}\), then it is contained in exactly \(\lambda\) blocks of \(\mathcal{A}'\), namely \(G\) (\(\lambda\) times). If \([x, y]\) is not contained in any group of \(\mathcal{D}\), then \([x, y]\) is contained in exactly \(\lambda\) blocks of \(\mathcal{A}\). Hence \(v + 1 \in B[M', X, \lambda]\).

Lemma 1.13. Let \(K, M \subseteq \mathbb{N}\) and \(k, \lambda, m \in \mathbb{N}\). Let \(n \in G[K, M, 1]\). Suppose that \(mk_1G[m, \lambda]\) for every \(k_1 \in K\) and that \(mn_1G[k, \lambda]\) for every \(m_1 \in M\). Then \(mn \in B[k, \lambda]\).

Proof: Let \(X = I_\mathbb{N} \times I_\mathbb{N}\). Let \((I_\mathbb{N}, \mathcal{A}, \mathcal{D})\) be an \((n, M, K, 1)\)-GDD. For every block \(B\) of this GDD, \(m\mid B\mid \in G[m, \lambda]\). Let \((I_\mathbb{N} \times B, \mathcal{A}, \mathcal{D})\) be such an \((m\mid B\mid, m, \lambda)\)-GDD, where 
\(\mathcal{A} = \{I_\mathbb{N} \times \{x\} \mid x \in B\}\). For every \(G \in \mathcal{D}\), \(m\mid G\mid \in B[k, \lambda]\). Let \((I_\mathbb{N} \times G, \mathcal{A}, \mathcal{D})\) be such a BIBD. Combine together all the entries of \(\mathcal{A}_B\) for every block \(B\) of \(\mathcal{A}\) and all the entries of \(\mathcal{A}_G\) for every group \(G \in \mathcal{D}\), and form a family. Let us call it \(\mathcal{D}\). Then we claim that \((X, \mathcal{D})\) is an \((mn, k, \lambda)\)-BIBD. Let \((i, j)\) and \((i', j')\) \(\in X\) such that \((i, j) \neq (i', j')\). If \(j = j'\), then \(j\) is
in a unique group $G \in \mathcal{J}$. But then $(i,j)$ and $(i',j)$ are in $\lambda$ blocks of the $(m|G|,k,\lambda)$-BIBD $(I_m \times G, \mathcal{A}_G)$. If $j \neq j'$, then either $j$ and $j'$ are in a unique group $G$ of $\mathcal{J}$ or they are in distinct groups of $\mathcal{J}$. In the first case, $(i,j)$ and $(i',j')$ are in $\lambda$ blocks of the $(m|G|,k,\lambda)$-BIBD $(I_m \times G, \mathcal{A}_G)$. In the second case, $j$ and $j'$ are in a unique block $B$ of $\mathcal{J}$ and hence, $(i,j)$ and $(i',j')$ are in $\lambda$ blocks of $\mathcal{A}_B$ since they are in distinct groups of the $(m|B|,(m),(k,\lambda))$-GDD $(I_m \times B, \mathcal{J}_B, \mathcal{A}_B)$. This establishes the claim.

Lemma 1.14. Let $m,k,\lambda \in \mathbb{N}$ and $K,M \subseteq \mathbb{N}$. Let $n \in G_{K[M,1]}$. Suppose that $mk_1 \in G_{(k)}[(m),\lambda]$ for every $k_1 \in K$ and that $mn + 1 \in B[k;\lambda]$ for every $m_1 \in M$. Then $mn + 1 \in B[k;\lambda]$.

Proof: Let $X = (I_m \times I_n) \cup \{\infty\}$ where $\infty$ is an additional point not in $I_m \times I_n$. Let $(I_m, \mathcal{J}, \mathcal{A})$ be an $(n,M,K,1)$-GDD. For every block $B$ of this GDD, $m|B| \in G_{(k)}[(m),\lambda]$. Let $(I_m \times B, \mathcal{J}_B, \mathcal{A}_B)$ be such an $(m|B|, (m),(k,\lambda))$-GDD where $\mathcal{J}_B = \{I_m \times \{i\} \mid i \in B\}$. For every $G \in \mathcal{J}, m|G| + 1 \in B[k;\lambda]$. Let $((I_m \times G) \cup \{\infty\}, \mathcal{A}_G)$ be such a BIBD. Combine together all the entries of $\mathcal{A}_B$ for every $B$ in $\mathcal{J}$ and all the entries of $\mathcal{A}_G$ for every $G \in \mathcal{J}$. The family consisting of all these blocks will be denoted by $\mathcal{B}$. Then we claim that $(X, \mathcal{B})$ is an $(mn + 1,k,\lambda)$-BIBD. Let $(i,j) \in I_m \times I_n$. Then $j$ is in a unique group of $\mathcal{J}$, say $G$. Then $(i,j)$ and $\infty$ are contained in exactly $\lambda$ blocks of the $(m|G| + 1,k,\lambda)$-BIBD.
\((I_m \times G) \cup [\omega], \mathcal{G}_G\). Using an argument similar to that used in the proof of Lemma 1.13, we see that the number of entires of \(G\) which contain 2 elements of \(I_m \times I_m\) is \(\lambda\).

Now let us examine some relations among the sets \(G_K[M,\lambda]\). First of all, it is clear to see that if \(M' \subseteq M\), and \(K' \subseteq K\), then \(G_{K'}[M',\lambda] \subseteq G_K[M,\lambda]\). We observe the following lemmas. Let \(\lambda, \lambda' \in \mathbb{N}, M, M', K, J \subseteq \mathbb{N}\).

**Lemma 1.15.** If \(\lambda' \mid \lambda\), then \(G_K[M,\lambda'] \subseteq G_K[M,\lambda]\).

**Proof:** Let \((X,\mathcal{X},\mathcal{G})\) be a \((v,M,K,\lambda')\)-GDD where \(v\) is an element of \(G_K[M,\lambda']\). Let \(\lambda = a\lambda'\) for some \(a \in \mathbb{N}\). Then take all the entries of \(\mathcal{G}\), each a times, and form the family \(\mathcal{G}'\). Then \((X,\mathcal{X},\mathcal{G}')\) is a \((v,M,K,\lambda')\)-GDD.

**Lemma 1.16.** If \(K \subseteq B[J;\lambda']\), then \(G_K[M,\lambda] \subseteq G_J[M,\lambda\lambda']\).

**Proof:** Let \(v \in G_K[M,\lambda]\) and \((X,\mathcal{X},\mathcal{G})\) be a \((v,M,K,\lambda')\)-GDD. Let \(\mathcal{G} = (B_i \mid i \in I)\). For every \(i \in I\), \(|B_i| \in K \subseteq B[J;\lambda']\).

Hence there is a \((|B_i|,J,\lambda_2)\)-PBD on \(B_i\), say \((B_i,\mathcal{G}_i)\) where \(\mathcal{G}_i = (B_{ij} \mid j \in J_i)\) for some indexing set \(J_i\). Let \(\mathcal{G}' = (B_{ij} \mid i \in I, j \in J_i)\). Then we claim that \((X,\mathcal{X},\mathcal{G}')\) is a \((v,M,J,\lambda\lambda')\)-GDD.

Indeed, for any 2-set \([x,y] \subseteq X\) such that \(x\) and \(y\) are in distinct groups of \(\mathcal{X}\), \([x,y] \subseteq B_{ij}\) for some \(i \in I\) and some \(j \in J_i\) iff \([x,y] \subseteq B_i\). The number of indices \(i \in I\) such
that \((x,y) \in B_i\) is \(\lambda\) and, for each such \(i \in I\), the number of indices \(j \in J_i\) such that \((x,y) \in B_{ij}\) is \(\lambda'\).

This technique will be referred to as 'breaking up blocks.' It follows very easily from Lemma 1.16 that \(G_{K'[M',\lambda]} = G_{B[K][M,\lambda]}\).

**Lemma 1.17.** If \(v \in G_{K[M',\lambda']}\) and \(M' \subseteq G_{K[M,\lambda]}\), then \(v \in G_{K[M,\lambda\lambda']\lambda'}\).

**Proof:** Let \((X,\mathcal{G}',\mathcal{A}')\) be a \((v,M',K',\lambda')\)-GDD and let
\[\mathcal{G} = \{G_i \mid i = 1, 2, \ldots, n\}.\]
For each \(i \in I_n\), \(|G_i| \in M' \subseteq G_{K[M,\lambda]}\) and hence, a \(|G_i|,M,K,\lambda\)-GDD exists, say \((G_i,\mathcal{A}_i,\mathcal{B}_i)\). Let
\[\mathcal{A}_1 = \{G_{ij} \mid j \in J_i\}\]
for some indexing set \(J_i\) and
\[\mathcal{A}_i = \{B_{ij} \mid i \in I_n\}\]
for some indexing set \(L_i\). Let
\[\mathcal{A} = \{G_i \mid i \in I_n, j \in J_i\}\]
and \(\mathcal{A}' = \{B_{ij} \mid i \in I_n, j \in L_i\}\). Now take each entry of \(\mathcal{A}'\), \(\lambda\) times, and each entry of \(\mathcal{A}''\), \(\lambda'\) times.

Form the family \(\mathcal{A}\), namely \(\lambda\mathcal{A}' + \lambda'\mathcal{A}''\). We claim that \((X,\mathcal{G}',\mathcal{A})\) is a \((v,M,K,\lambda\lambda')\)-GDD.

Let \((x,y) \subseteq X\) be any 2-set such that \(x\) and \(y\) are in distinct groups \(G_{ij}\)'s. Then either they are in \(G_i\) for some \(i \in I_n\) or they are in distinct \(G_{ij}\)'s. In the first case, the number of indices \(\ell \in L_i\) such that \((x,y) \in B_{i\ell}\) is \(\lambda\) in the GDD \((G_i,\mathcal{A}_i,\mathcal{B}_i)\). In the second case, \((x,y)\) is not contained in any entries of \(\mathcal{A}''\) and it is contained in \(\lambda'\) entries of \(\mathcal{A}'\). By the definition of \(\mathcal{A}\), we have the result.
This technique will be referred to as 'breaking up groups.' It follows very easily from the proof of Lemma 1.17 that if
\( v \in G'_{K}[M',\lambda] \) and \( M' \subseteq G_{K}[M,\lambda] \), then \( v \in G_{K}[M,\lambda] \). We now prove a very important and useful theorem. It is a generalization of a theorem in [26], where the index of pairwise balance is one. Following the convention in [26], we define a weighting of a GDD \((X,\mathscr{B},\mathscr{A})\) to be a mapping \( w: X \rightarrow \mathbb{N}_0 \) which assigns to each point of \( X \) a nonnegative weight.

**Theorem 1.18 (GDD Composition Theorem).** Let \((X,\mathscr{B},\mathscr{A})\) be a GDD with index of pairwise balance \( \lambda_1 \) and let \( w \) be a weighting on \( X \). Assume that for each entry \( B \) of \( \mathscr{A} \), there is a GDD with group type \( (w(x) \mid x \in B, w(x) \neq 0), \) block sizes from \( K \), and index of pairwise balance \( \lambda_2 \). Then we may construct a certain GDD \((X^*,\mathscr{B}^*,\mathscr{A}^*)\) with block sizes from \( K \), group type
\[
(\sum_{x \in X} w(x) \mid G \in \mathscr{B}, \sum_{x \in G} w(x) \neq 0),
\]
and index of pairwise balance \( \lambda_1 \lambda_2 \).

**Proof:** For every \( x \in X \), let \( M_x \) be a set of \( w(x) \) elements such that \( M_x \cap M_y = \emptyset \) for \( x \neq y \). Put \( G^* = \bigcup_{x \in G} M_x \) for every \( G \in \mathscr{B} \). Let \( \mathscr{B}^* = \{G^* \mid G \in \mathscr{B}, G^* \neq \emptyset\} \) and \( X^* = \bigcup_{x \in X} M_x \). For every entry \( B \) of \( \mathscr{A} \), we have a GDD with group type \( (w(x) \mid x \in B, w(x) \neq 0), \) block sizes from \( K \), and index of pairwise balance \( \lambda_2 \). Let \( (\bigcup_{x \in B} M_x,\mathscr{B}_B,\mathscr{A}_B) \) be one
such GDD where $\mathcal{X}_B = \{ M_x \mid x \in B, M_x \neq \emptyset \}$. Take all the entries of $\mathcal{X}_B$ for every entry $B$ of $\mathcal{X}$ and form a family and denote it by $\mathcal{X}_B^*$. Then we claim that $(x^*, y^*, \mathcal{X}_B^*)$ is a GDD with block sizes from $K$, group type $(\Sigma w(x) \mid G \in \mathcal{X}, \Sigma w(x) \neq 0)$, and index of pairwise balance $\lambda_1 \lambda_2$.

Clearly, it has the correct group type and its block sizes are from $K$. A 2-set $(x, y) \subseteq X^*$ is contained in a group $G^*$ of $\mathcal{X}$ iff (i) for some $a \in G$, $(x, y) \subseteq M_a$ or (ii) for some 2-set $(a, b) \subseteq G$, $x \in M_a$ and $y \in M_b$. Let $(x, y) \subseteq X^*$ be any 2-set such that $x$ and $y$ are not contained in a group of $\mathcal{X}_B^*$. Then there exist $a$ and $b$ of $X$, not in a group of $\mathcal{X}$, such that $x \in M_a$ and $y \in M_b$. Since $(X, \mathcal{X}, \mathcal{X}_B)$ is a GDD with index of pairwise balance $\lambda_1$, $(a, b)$ is contained in exactly $\lambda_1$ blocks of $\mathcal{X}$, say $B_1, B_2, \ldots, B_{\lambda_1}$. Now for each $i = 1, 2, \ldots, \lambda_1$, $(x, y) \subseteq \bigcup_{x \in B_i} M_x$ is a 2-set and hence, by assumption, it is contained in exactly $\lambda_2$ blocks of the GDD $(\bigcup_{x \in B_i} \mathcal{X}_B^*, \mathcal{X}_B^*).$ Hence $(x, y)$ is contained in exactly $\lambda_1 \lambda_2$ blocks, as claimed.

Let us consider a special kind of GDD's in which all groups have the same size, i.e. with group type $n \cdot [m]$ for some $n, m \in \mathbb{N}$. Define the set

$$\text{NG}[m, K, \lambda] = \{ n \in \mathbb{N} \mid \text{there exists a GDD with } n \text{ groups of size } m, \text{ block sizes from } K, \text{ and index of pairwise balance } \lambda \}.$$
This notation is a slight generalization of that introduced in [26] where $\lambda = 1$. (NG stands for 'number of groups.') Thus, $n \in NG[m,K,\lambda]$ iff $nm \in G_k([m,\lambda])$. Recall that if $(X,\sigma)$ is a PBD then $(\bar{X},\bar{\sigma})$ is a GDD where $\bar{X} = \{(x)|x \in X\}$. Thus, we have $B[K;\lambda] = NG[1,K,\lambda]$. With this in mind, we have the following corollaries of Theorem 1.18.

**Corollary 1.19.** $NG[m_1,NG[m_2,K,\lambda_2],\lambda_1] \subseteq NG[m_1m_2,K,\lambda_1\lambda_2]$.

**Proof:** Let $(X,\lambda,\sigma)$ be a $(nm_1,\{m_1\},NG[m_2,K,\lambda_2],\lambda_1)$-GDD where $n \in NG[m_1,NG[m_2,K,\lambda_2],\lambda_1]$. Let $w:X \rightarrow \mathbb{N}_0$ be defined as $w(x) = m_2$ for every $x \in X$. For each block $B$ of $\sigma$, $|B| \in NG[m_2,K,\lambda_2]$. i.e. a $(|B|m_2,\{m_2\},K,\lambda_2)$-GDD exists. By Theorem 1.18, we have the result.

Taking $m_1 = 1$ in Corollary 1.19 and recalling $B[K;\lambda] = NG[1,K,\lambda]$, we have

**Corollary 1.20.** $B[NG[m,K,\lambda];\lambda'] \subseteq NG[m,K,\lambda\lambda'].$

Taking $\lambda' = 1$ in Corollary 1.20, we have

**Corollary 1.21.** $B[NG[m,K,\lambda]] = NG[m,K,\lambda]$, (i.e. $NG[m,K,\lambda]$ is a closed set).

We shall write $NG[m,K]$ instead of $NG[m,K,1]$, $NG[m,k,\lambda]$ instead of $NG[m,(k),\lambda]$, and $NG[m,k]$ for $NG[m,(k),1]$. Now taking $\lambda = 1$ in Corollary 1.20, we have
Corollary 1.22. \( B[NG[m,K] ; \lambda] \subseteq NG[m,K,\lambda] \).

Taking \( m_2 = 1 \) in Corollary 1.19, we have

Corollary 1.23. \( NG[m,B[K;\lambda_2,\lambda_1]] \subseteq NG[m,K,\lambda_1\lambda_2] \).

This is actually a special case of Lemma 1.16, breaking up blocks.

From now on, we will restrict ourselves to the GDD's in which all groups have the same size, i.e. with group type \( n \cdot \{m\} \) for some \( n,m \in \mathbb{N} \). We shall denote it by \( GD(n,m,K,\lambda) \). Write \( GD(n,m,k,\lambda) \) instead of \( GD(n,m,K,\lambda) \), \( GD(n,m,K) \) instead of \( GD(n,m,K,\lambda) \), and \( GD(n,m,k) \) instead of \( GD(n,m,K,\lambda) \). Naturally, one would like to determine the quadruples \( (n,m,K,\lambda) \) for which a \( GD(n,m,K,\lambda) \) exists.

\( (I_m,[I_m],\emptyset) \) is clearly a \( GD(1,m,K,\lambda) \). Hence \( 1 \in NG[m,K,\lambda] \). If \( 2 \in K \), \( GD(n,m,K,\lambda) \) exists for any \( n,m \in \mathbb{N} \) and any \( K \subseteq \mathbb{N} \). Indeed, take all the pairs which are not in a group of \( \emptyset \). Here \( \lambda = an(n - 1)m^2 \) for some \( a \in \mathbb{N} \). Also, it is clear to see that \( NG[m,K,1] = NG[m,K \cup \{1\},1] \). Therefore, without loss of generality, we may assume from now on that \( k \geq 3 \) for every \( k \in K \). It is clear from the definition of a GDD that in a GDD, \( n \geq \min(K) \).

Now let us find out the necessary conditions for the existence of a \( GD(n,m,K,\lambda) \).

Proposition 1.24. Let \( m,\lambda \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \). If \( n \in NG[m,K,\lambda] \), then

\[
\lambda n(n - 1)m^2 \equiv 0 \pmod{\beta(K)}, \quad \text{and} \quad (1.7)
\]
\[ \lambda(n - 1)m \equiv 0 \pmod{\alpha(K)}. \]

**Proof:** Let \((X, \mathcal{J}, \mathcal{A})\) be a GD\((n, m, K, \lambda)\). Let \(\mathcal{A} = \{B_i | i \in I\}\) and \(\mathcal{J} = \{G_j | j \in I_n\}\). Let us define its incidence relation \(\rho\), for \(x \in X\) and \(i \in I\), by

\[
\rho(x, B_i) = \begin{cases} 
1 & \text{if } x \in B_i, \\
0 & \text{if } x \notin B_i.
\end{cases}
\]

For any 2-set \(\{x, y\} \subseteq X\) such that \(x\) and \(y\) are in distinct groups of \(\mathcal{J}\), we have by the definition of a GDD that

\[
\lambda = \sum_{i \in I} \rho(x, B_i) \rho(y, B_i)
\]

and hence,

\[
\lambda(n - 1)m^2 = \sum_{\substack{x \in G_{j_i}, y \in G_{j_j}, i \in I \\text{ or } j \neq j' \in I_n}} \rho(x, B_i) \rho(y, B_i).
\]

Interchanging the order of summation, we get

\[
\lambda(n - 1)m^2 = \sum_{i \in I} \sum_{\substack{x \notin y \in X}} \rho(x, B_i) \rho(y, B_i).
\]

But for every \(i \in I\), the inner sum is \(|B_i|(|B_i| - 1) \equiv 0 \pmod{\beta(K)}\).

Hence,

\[
\lambda(n - 1)m^2 \equiv 0 \pmod{\beta(K)}.
\]

Let \(x_o \in X\) be any fixed element belonging to \(G_{j_o}\). Let \(y \in X\) such that \(x_o \neq y\) and that they are in distinct groups of \(\mathcal{J}\). Then we have, by definition of a GDD, \(\lambda = \sum_{i \in I} \rho(x_o, B_i) \rho(y, B_i)\).
and hence,

\[ \lambda(n - 1)m = \sum_{y \in G_j} \sum_{\substack{i \in I \setminus \{j\} \setminus \{j\} \setminus \{i\} \setminus \{n\} \setminus \{o\}}} \rho(x_o, B_i) \rho(y, B_i) \cdot \]

Interchanging the order of summation, we get

\[ \lambda(n - 1)m = \sum_{i \in I} \rho(x_o, B_i) \sum_{y \in X, y \neq x_o} \rho(y, B_i) \cdot \]

i.e.

\[ \lambda(n - 1)m = \sum_{i \in I} \rho(x_o, B_i) \sum_{y \in X - \{x_o\}} \rho(y, B_i) \cdot \]

But, if \( \rho(x_o, B_i) \neq 0 \), then the inner sum is \( |B_i| - 1 \equiv 0 \pmod{\alpha(K)} \). Hence,

\[ \lambda(n - 1)m \equiv 0 \pmod{\alpha(K)} \cdot \]

One would naturally ask whether or not (1.7) and (1.8) are sufficient for \( n \in NG[m, K, \lambda] \). Hanani [16] showed that when \( K = \{3\} \), (1.7) and (1.8) are sufficient for \( n \in NG[m, 3, \lambda] \). One of our main results is that, for fixed \( m, K, \) and \( \lambda, \) (1.7) and (1.8) are actually 'asymptotically sufficient' for \( n \in NG[m, K, \lambda] \). Also we will include an independent proof for the case \( K = \{3\} \) and \( \lambda = 1 \).

§1.4 Transversal Designs and Lattice Designs.

The most important and useful GDD's are GD(k, m, k, l), i.e. those with \( k \) groups of size \( m \), block size \( k \) and index of pairwise balance = 1. We will denote such a GDD by TD(k, m, l)
and call it transversal design. In general, a GD(k,m,k,\lambda) will be called a transversal design with group size m, block size k, and index of pairwise balance \lambda and will be denoted by TD(k,m,\lambda). Thus, TD(k,m,\lambda) exists iff \text{NG}[m,k,\lambda]. TD(k,m,\lambda) has a property that every block intersects every group in precisely one point.

Write TD(k,m) for TD(k,m,1). It is a well-known theorem (see [10]) that the existence of a TD(k,m) is equivalent to the existence of \text{k - 2 mutually orthogonal Latin squares of order m} which in turn is equivalent to the existence of an \text{(m^2,k,m,2)} orthogonal array of strength 2. With TD(k,m)'s one can construct a number of other GDD's. For example, suppose TD(k,m) exists and TD(k,km) exists. By breaking up the groups of TD(k,km) (Lemma 1.17), we have k^2 \in \text{NG}[m,k]. Define the set

\[ OA[k,\lambda] = \{ m \in \mathbb{N} \mid \text{TD}(k,m,\lambda) \text{ exists} \}. \]

We shall write OA[k] for OA[k,1]. Let us observe some relations among the sets OA[k,\lambda].

**Proposition 1.25.** If \lambda' \mid \lambda, then OA[k,\lambda'] \subseteq OA[k,\lambda].

**Proof:** Let (X,\mathcal{S},\mathcal{A}) be a TD(k,m,\lambda') where m \in OA[k,\lambda']. Take all the entries of \mathcal{A}, each a\lambda times where \lambda = a\lambda'. Then form a family. Let it be denoted by \mathcal{A}'. Then (X,\mathcal{S},\mathcal{A}') is a TD(k,m,\lambda).
Proposition 1.26. If \( k' \leq k \), then \( OA[k, \lambda] \subseteq OA[k', \lambda] \).

Proof: Let \( m \in OA[k, \lambda] \). Let \((X, \mathcal{A})\) be a \( TD(k, m, \lambda) \).
Let \( \mathcal{A} = \{G_1, G_2, \ldots, G_k\} \) where \( |G_i| = m \) for every \( i \in I_k \).
Let \( S = \bigcup_{i=k+1}^{k} G_i \). Let \( X' = X - S \) and \( \mathcal{A}' = \{G_1, G_2, \ldots, G_k\} \).

For every \( B \) of \( \mathcal{A} \), let \( B' = B - (B \cap S) \). Let \( \mathcal{A}' = (B_i | i \in I) \).
Put \( \mathcal{A}' = (B_i | i \in I) \). Then it is easy to see that \((X', \mathcal{A}', \mathcal{A}')\) is a \( TD(k', m, \lambda) \).

It is clear from the definition that \( TD(k, m, \lambda) \) exists iff \( k \in NG[m, k, \lambda] \). As a corollary of Corollary 1.19, we have

Proposition 1.27. If \( m_1 \in OA[k, \lambda_1] \) and \( m_2 \in OA[k, \lambda_2] \), then \( m_1 m_2 \in OA[k, \lambda_1 \lambda_2] \).

Proof: \( m_2 \in OA[k, \lambda_2] \) iff \( TD(k, m_2, \lambda_2) \) exists iff \( k \in NG[m_2, k, \lambda_2] \). But \( NG[m, k, \lambda] \subseteq NG[m, J, \lambda] \) if \( K \subseteq J \).
Similarly, one has \( m_1 \in OA[k, \lambda_1] \) iff \( k \in NG[m_1, k, \lambda_1] \subseteq NG[m_1, NG[m_2, k, \lambda_2], \lambda_1] \). By Corollary 1.19, we have \( k \in NG[m_1 m_2, k, \lambda_1 \lambda_2] \), i.e. \( m_1 m_2 \in OA[k, \lambda_1 \lambda_2] \).

If \( TD(k, m, \lambda_1) \) and \( TD(k, m, \lambda_2) \) exist, then \( TD(k, m, n_1 \lambda_1 + n_2 \lambda_2) \) exists for any \( n_1, n_2 \in \mathbb{N} \). Let \((X, \mathcal{A}_1)\) be a \( TD(k, m, \lambda_1) \) and \((X, \mathcal{A}_2)\) a \( TD(k, m, \lambda_2) \). Then, putting \( \mathcal{A} = n_1 \mathcal{A}_1 + n_2 \mathcal{A}_2 \), we have that \((X, \mathcal{A})\) is a \( TD(k, m, n_1 \lambda_1 + n_2 \lambda_2) \). Much work is done on \( OA[k] \). Chowla, Erdös, and Straus [8] using the results of Bose, Shrikhande, and Parker [5], have proved that there exists a
constant \( c(k) \) such that \( m \in \text{OA}[k] \) for all \( m > c(k) \). Let \( \text{oa}(k) \) denote the smallest integer such that \( m \in \text{OA}[k] \) for all \( m > \text{oa}(k) \). Then one of the remarkable results of [5] is that \( \text{oa}(4) = 6 \). In terms of Latin squares, there exists a pair of mutually orthogonal Latin squares of order \( m \) for \( m \neq 2, 6 \).

Hanani [14] proved that \( \text{oa}(7) \leq 62 \). Wilson [29] proved that \( \text{oa}(5) \leq 46 \), \( \text{oa}(6) \leq 60 \), and \( \text{oa}(8) \leq 90 \). It is also well-known that

Proposition 1.28. If \( k \) is a prime power, then \( k \in \text{OA}[k] \).

Proof: Let \( X = GF(k) \times GF(k) \), \( G_a = GF(k) \times \{a\} \) for \( a \in GF(k) \), and \( \mathcal{A} = \{G_a \mid a \in GF(k)\} \). For \( b, c \in GF(k) \), let \( \mathcal{B}_{b,c} = \{(b + ac, a) \mid a \in GF(k)\} \). Put \( \mathcal{A} = \{\mathcal{B}_{b,c} \mid b, c \in GF(k)\} \).

We claim that \((X, \mathcal{A})\) is a TD(k,k). Let \((d_1, a_1)\) and \((d_2, a_2)\) \( \in X \) be two elements of \( X \) belonging to different groups. It is easy to see that \( a_1 \neq a_2 \). But the system of linear equations in \( b \) and \( c \)

\[
\begin{cases}
 b + a_1 c = d_1 \\
 b + a_2 c = d_2 
\end{cases}
\]

has a unique solution in \( b, c \) since \( a_1 \neq a_2 \). That is, the number of blocks which contain \((d_1, a_1)\) and \((d_2, a_2)\) is exactly one. Hence \( k \in \text{OA}[k] \).

Let \( \mathcal{A}_C = \{\mathcal{B}_{b,c} \mid b \in GF(k)\} \). Let \((x, y) \in X\) be any point. Then there is a unique \( b \) such that \( b + yc = x \). Hence
$(x,y) \in B_{b,y}$ and $\mathcal{A}_c$ partitions $X$. In fact $\mathcal{A} = \bigcup_{c \in GF(k)} \mathcal{A}_c$ is a partition of $\mathcal{A}$. This leads us to the following definition.

A TPD$(k,m)$ (transversal design with one parallel class) is a quadruple $(X,\mathcal{A}_1,\mathcal{A},\mathcal{A}')$ such that $(X,\mathcal{A}_1,\mathcal{A}_1 \cup \mathcal{A}')$ is a TD$(k,m)$ and $\mathcal{A}_1$ is a parallel class of blocks. $(X,\mathcal{A})$ is said to be resolvable iff $\mathcal{A}$ can be partitioned into parallel classes. Let us observe that if $(X,\mathcal{A})$ is a resolvable TD$(k,m)$, then the number of parallel classes, into which $\mathcal{A}$ can be partitioned, is $m$. In fact, if $G$ is a group and $x_0 \in X - G$, then $\{x,x_0\}$ is in a unique block for every $x \in G$. Thus, we have $m$ blocks containing $x_0$. Each parallel class must contain exactly one such block. So, the number of parallel classes is $m$, i.e. if $(X,\mathcal{A})$ is a resolvable TD$(k,m)$, then $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \cdots \cup \mathcal{A}_m$ where $\mathcal{A}_i$ is a parallel class on $X$ and they partition $\mathcal{A}$.

Let $\text{OAT}^R[k] = \{m \in \mathbb{N} \mid \text{a TPD}(k,m) \text{ exists}\}$ and $\text{OAR}^R[K] = \{m \in \mathbb{N} \mid \text{a resolvable TD}(k,m) \text{ exists}\}$. Then,

Proposition 1.29. $\text{OAR}[k + 1] = \text{OAR}^R[k] \subseteq \text{OAT}^T[k] \subseteq \text{OAT}[k]$.

Proof: Let $(X,\mathcal{A},\mathcal{A})$ be a resolvable TD$(k,m)$ where $m \in \text{OAR}^R[k]$, say $\mathcal{A} = \mathcal{A}_1 \cup \mathcal{A}_2 \cup \cdots \cup \mathcal{A}_m$. Let $\varphi$ be a one-to-one mapping $\{\mathcal{A}_1,\mathcal{A}_2, \ldots, \mathcal{A}_m\} \rightarrow M$ where $M$ is an $m$-set such that $M \cap X = \emptyset$. Assume $\varphi(\mathcal{A}_i) = a_i \in M$ for $i \in I_m$. Let $X' = X \cup M$. Let $\mathcal{A}_i' = \mathcal{A} \cup \{a_i\}$ for $i \in I_m$. Let $\mathcal{A}_i' = \mathcal{A}_i \cup \{a_i\}$ for $i \in I_m$. Put $\mathcal{A}' = \bigcup_{i \in I_m} \mathcal{A}_i'$. Then it is clear that $(X',\mathcal{A}',\mathcal{A}')$ is a
TD(k + 1, m), since \( \mathcal{A}_1 \) is a parallel class on \( X \).

Conversely, let \((X, \mathcal{S}, \mathcal{A})\) be a TD(k + 1, m), say
\[
\mathcal{S} = \{G_1, \ldots, G_k, G_{k+1}\}.
\]
Let \( X' = X - G_{k+1} \) and \( \mathcal{S}' = \{G_1, G_2, \ldots, G_k\} \). Put \( \mathcal{A}' = \{B \cap (X - G_{k+1}) \mid B \in \mathcal{A}\} \). Then we claim that \((X', \mathcal{S}', \mathcal{A}')\) is a resolvable TD(k, m). \((X', \mathcal{S}', \mathcal{A}')\) is clearly a TD(k, m). For every \( a \in G_{k+1} \), define
\[
\mathcal{A}'_a = \{A - \{x_0\} \mid x_0 \in A \in \mathcal{A}\}.
\]
Clearly, \( \mathcal{A}'_a \) is a parallel class on \( X \) and \( \{\mathcal{A}'_a \mid a \in G_{k+1}\} \) partitions \( \mathcal{A} \).

In view of Propositions 1.28 and 1.29, we have

**Proposition 1.30.** If \( k \) is a prime power, then \( k \in OA[k + 1] \).

In view of Propositions 1.26, 1.27, and 1.30, we have the well-known theorem [19],

**Theorem 1.31 (MacNeish).** Let \( m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \) be the factorization of \( m \) into powers of distinct primes. Then \( m \in OA[k] \) where \( k = 1 + \min(p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}) \).

We now state one of the remarkable results in [29].

**Theorem 1.32.** There exists a positive integer \( k_o \) such that if \( k > k_o \), then, for every \( m > k^{17} \), \( m \in OA[k] \).

Let \( X \) be a given \( km \)-set. Let \((X, \mathcal{A}_1, \mathcal{S}, \mathcal{A})\) be a TPD(k, m) on \( X \). Then both \( \mathcal{S} \) and \( \mathcal{A}_1 \) partition \( X \).

\(|G \cap B| = 1\) for every \( G \in \mathcal{S} \) and every \( B \in \mathcal{A}_1 \). No block of
\( \mathcal{A} \) meets \( G \) or \( B \) in more than one point of \( X \) for any \( G \in \mathcal{G} \) and any \( B \in \mathcal{A}_1 \). For every 2-set \( \{x, y\} \) of \( X \) such that \( \{x, y\} \) is not contained in a group \( G \) of \( \mathcal{G} \) and is not contained in any block of \( \mathcal{A}_1 \), \( \{x, y\} \) is contained in a unique block \( \mathcal{A} \). These properties are actually the properties of the following combinatorial structure.

**Definition.** Let \( n, m, \lambda \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \). An \((n, m, K, \lambda)\)-LD (lattice designs on \( nm \) points, with vertical group size \( n \), horizontal group size \( m \), block sizes from \( K \), and index of pairwise balance \( \lambda \)) is a quadruple \((X, \mathcal{V}, \mathcal{W}, \mathcal{A})\) where

1. \( X \) is a finite set of \( nm \) points,
2. \( \mathcal{V} \) is a class of \( n \)-subsets of \( X \) which partition \( X \),
3. \( \mathcal{W} \) is a class of \( m \)-subsets of \( X \) which partition \( X \),
4. \( |V \cap H| = 1 \) for every \( V \in \mathcal{V} \) and every \( H \in \mathcal{W} \),
5. \( \mathcal{A} \) is a family of subsets of \( X \), say \((B_i | i \in I)\) for some indexing \( I \), such that \( |B_i| \in K \),
6. \( |B_i \cap V| \leq 1 \) and \( |B_i \cap H| \leq 1 \) for every \( i \in I \), every \( V \in \mathcal{V} \) and every \( H \in \mathcal{W} \),
7. for every 2-set \( \{x, y\} \subseteq X \) such that \( x \) and \( y \) are not in some \( H \in \mathcal{W} \) or some \( V \in \mathcal{V} \), the number of indices \( i \in I \) such that \( \{x, y\} \subseteq B_i \) is precisely \( \lambda \).

The elements of \( X \) will be called points or treatments, the elements of \( \mathcal{A} \) will be called blocks or lines, the elements of \( \mathcal{V} \)
will be called vertical groups, and the elements of will be called horizontal groups. We shall denote an \((n,m,K,\lambda)\)-LD by \(LD(n,m,K,\lambda)\). Write \(LD(n,m,K)\) instead of \(LD(n,m,K,\lambda)\), \(LD(n,m,k,\lambda)\) instead of \(LD(n,m,(k),\lambda)\), and \(LD(n,m,k)\) instead of \(LD(n,m,(k),1)\). Clearly, \(LD(n,m,K,\lambda)\) exists iff \(LD(m,n,K,\lambda)\) exists (by exchanging the roles of vertical and horizontal groups). We also note that a TPD\((k,m)\) is nothing but an \(LD(k,m,k)\).

LD's were first introduced in [5] (although with a different terminology) and were used to construct GDD's. In fact, one of the constructions in [5] is a special case of the following proposition.

**Proposition 1.33.** Let \(n,m,\lambda,\lambda' \in \mathbb{N}\), and \(J,M,K \subseteq \mathbb{N}\). Let \((X,\mathcal{A})\) be a GDD on \(m\) points, with block sizes from \(J\), group sizes from \(M\), and index of pairwise balance \(\lambda\). Suppose that, for every group \(G\) of \(\mathcal{A}\), a GDD\((n,|G|,K,\lambda')\) exists and that, for every block \(B\) of \(\mathcal{A}\), an LD\((n,|B|,K,\lambda')\) exists. Then a GDD\((n,m,K,\lambda\lambda')\) exists.

**Proof:** Let \(X^* = X \times I_n\), \(X_i = X \times \{i\}\) for every \(i \in I_n\), and \(\mathcal{J}^* = \{X_1, \ldots, X_n\}\). For every \(G \in \mathcal{A}\), let \(G^* = G \times I_n\), \(G_i = G \times \{i\}\) for every \(i \in I_n\), and \(\mathcal{J}_G = \{G_1, G_2, \ldots, G_n\}\). Let \((G^*,\mathcal{J}_G,\mathcal{A}_G)\) be a GDD\((n,|G|,K,\lambda')\). For every block \(B\) of \(\mathcal{A}\), let \(B^* = B \times I_n\). By assumption, an LD\((n,|B|,K,\lambda')\) exists on \(B^*\).

Without loss of generality, we may assume that \(B_i = B \times \{i\}\) for \(i \in I_n\) are the horizontal groups and that \(V_B^B = \{b\} \times I_n\) for \(b \in B\) are the vertical groups. Put \(V_B = \{V_B^B | b \in B\}\) and...
\[ \mathcal{B}_B = \{ B_i \mid i \in I_n \} \]. Let \((B^*, \gamma_B, \mathcal{B}_B, \mathcal{A}_B^*)\) be an \(LD(n, \lVert B \rVert, K, \lambda')\).

Take all the entries of \(\mathcal{A}_B^*\) for every block \(B\) of \(\mathcal{A}\) and form them a family, say \(\mathcal{A}''\). Then let \(\mathcal{A}^* = \sum_{G \in \mathcal{G}} \lambda \mathcal{A}_G + \mathcal{A}''\). We claim that \((X^*, \mathcal{G}^*, \mathcal{A}^*)\) is a \(GD(n, m, K, \lambda \lambda')\).

Clearly, it has the correct block size, vertical group size and vertical group size. Let \((x, i)\) and \((y, j)\) \(\in X^*\) be any two distinct points, not contained in the same group, i.e. \(i \neq j\).

If \(x = y\), then \(x\) is in a unique group, say \(G\) of \(\mathcal{G}\).

Therefore, in \((G^*, \mathcal{G}_G, \mathcal{A}_G)\), \((x, i)\) and \((x, j)\) are contained in exactly \(\lambda'\) blocks of \(\mathcal{A}_G\) and, hence, are contained in exactly \(\lambda \lambda'\) blocks of \(\mathcal{A}^*\). Hence we may assume that \(x \neq y\). But then they either are contained in a unique group of \(\mathcal{G}\) or are not contained in any group of \(\mathcal{G}\). In the first case, use the same argument as in the case \(x = y\). In the second case, \(x\) and \(y\) are contained in exactly \(\lambda\) blocks of \(\mathcal{A}\), say \(B_1, B_2, \ldots, B_{\lambda}\). Then, for each of these blocks, \((x, i)\) and \((y, j)\) are contained in exactly \(\lambda'\) blocks of the \(LD\) corresponding to the block \(B_1\). Hence \((x, i)\) and \((y, j)\) are contained in exactly \(\lambda \lambda'\) blocks of \(\mathcal{A}^*\).

In order to study the structures of \(LD(n, m, K, \lambda)\), let us define, for \(n, m, \lambda \in \mathbb{N}\) and \(K \subseteq \mathbb{N}\), the sets

\[ \text{NHG}[m, K, \lambda] = \{ v \in \mathbb{N} \mid \text{an LD}(v, m, K, \lambda) \text{ exists} \} \],

and

\[ \text{NVG}[n, K, \lambda] = \{ u \in \mathbb{N} \mid \text{an LD}(n, u, K, \lambda) \text{ exists} \} \].
(Here, 'NHG' stands for the number of horizontal groups and 'NVG' stands for the number of vertical groups.)

As an easy observation, we have $n \in \text{NHG}[m,K,\lambda]$ iff $m \in \text{NVG}[n,K,\lambda]$. We shall write $\text{NHG}[m,k,\lambda]$ instead of $\text{NHG}[m,(k),\lambda]$, $\text{NHG}[m,K]$ instead of $\text{NHG}[m,K,1]$, and $\text{NHG}[m,k]$ instead of $\text{NHG}[m,(k),1]$. Similarly, we shall adopt these conventions for $\text{NVG}[n,K,\lambda]$. Let us examine the relation of the sets $\text{NHG}[m,K,\lambda]$ ($\text{NVG}[n,K,\lambda]$) with the closure operation $B$.

**Proposition 1.34.** Let $m, \lambda, \lambda' \in \mathbb{N}$ and $K \in \mathbb{N}$. Then $B[\text{NHG}[m,K,\lambda];\lambda'] \subseteq \text{NHG}[m,\lambda,\lambda']$.

**Proof:** Let $n \in B[\text{NHG}[m,K,\lambda];\lambda']$. Let $(X,\mathcal{A})$ be an $(n,\text{NHG}[m,K,\lambda],\lambda')$ - PBD. Let $X^* = I_m \times X$, $V_i = \{i\} \times X$ for $i \in I_m$, $H_x = I_m \times \{x\}$ for $x \in X$, $\gamma^* = \{V_i \mid i \in I_m\}$ and $H^* = \{H_x \mid x \in X\}$. For every block $B$ of $\mathcal{A}$, $|B| \in \text{NHG}[m,K,\lambda]$, i.e. an $\text{LD}(|B|,m,K,\lambda)$ exists. Let $(I_m \times B, \gamma_B, H_B, \mathcal{A}_B)$ be such an LD where $\gamma_B = \{(i) \times B \mid i \in I_m\}$ and $H_B = \{I_m \times \{x\} \mid x \in B\}$. For convenience, let us write $\mathcal{A} = (B_i \mid i \in I)$ and $\mathcal{A}_{B_i} = (B_{ij} \mid j \in J_i)$ for some indexing sets $I$ and $J_i$'s. Let $\mathcal{A}^* = (B_{ij} \mid i \in I, j \in J_i)$. Then we claim that $(X^*, \gamma^*, H^*, \mathcal{A}^*)$ is an $\text{LD}(n,m,K,\lambda,\lambda')$.

Everything except (vii) in the definition for an LD is easily verified. To prove (vii), let $(i,x)$ and $(j,y)$ be two elements of $x^*$ such that $i \neq j$ and $x \neq y$. Then $x$ and $y$ are in exactly $\lambda'$ blocks of $\mathcal{A}$, say $B_1, B_2, \ldots, B_{\lambda'}$. For
each of these blocks, \((i,x)\) and \((j,y)\) are in \(I_m \times B\) and not in a vertical or horizontal group of the \(LD(I_m \times B, \mathcal{V}_B, \mathcal{H}_B, \mathcal{A}_B)\).

Hence they are contained in exactly \(\lambda\) blocks of this \(LD\).

Thus, they are contained in exactly \(\lambda \lambda'\) block of \(\mathcal{A}^*\), as claimed.

Similarly, one would have the following proposition (by exchanging the roles of the horizontal and vertical groups).

**Proposition 1.34'.** Let \(n, \lambda, \lambda' \in \mathbb{N}\) and \(K \subseteq \mathbb{N}\). Then \(B[NVG[n,K,\lambda]; \lambda'] \subseteq NVG[n,K,\lambda']\).

Let \(\lambda' = 1\) in Propositions 1.34 and 1.34'. We have the following important fact.

**Corollary 1.35.** Let \(n,m,\lambda \in \mathbb{N}\) and \(K \subseteq \mathbb{N}\). Then both \(NHG[m,K,\lambda]\) and \(NVG[n,K,\lambda]\) are closed sets (with respect to the closure operation \(B\)).

One would naturally like to find all the quadruples \((n,m,K,\lambda)\) for which an \(LD(n,m,K,\lambda)\) exists. Clearly, \((I_m, \mathcal{H}_m, \{I_m\}, \emptyset)\) is an \(LD(1,m,K,\lambda)\) where \(\mathcal{H}_m = \{\{i\} \mid i \in I_m\}\). Thus \(1 \in NHG[m,K,\lambda]\).

Similarly, \(1 \in NVG[n,K,\lambda]\). If \(2 \in K\), then take all 2-sets of \(I_m \times I_n\) which are contained in a vertical or horizontal group, namely \((i) \times I_n\) for \(i \in I_m\) and \(I_m \times (j)\) for \(j \in I_n\). Here, the index of pairwise balance is \(\lambda = an(n - 1)m(m - 1)\) for some \(a \in \mathbb{N}\). Also, it is easy to see that \(NHG[m,K,\lambda] = NHG[m,K \cup \{1\}, \lambda]\) (similarly for \(NVG[n,K,\lambda]\)). Therefore, without loss of generality,
we may assume from now on that \( k \geq 3 \) for every \( k \in K \). It is clear from the definition of an LD that \( \min(n,m) \geq \min(K) \).

Now let us find out the necessary conditions for the existence of an LD\((n,m,K,\lambda)\).

**Proposition 1.36.** Let \( m, \lambda \in \mathbb{W} \) and \( K \subseteq \mathbb{W} \). If \( n \in \text{NHG}[m,K,\lambda] \), then

\[
\lambda n(n - 1)m(m - 1) \equiv 0 \pmod{\beta(K)}, \quad \text{and} \quad (1.9)
\]

\[
\lambda(n - 1)(m - 1) \equiv 0 \pmod{\alpha(K)}. \quad (1.10)
\]

**Proof:** Let \((X,y,N,\mathcal{A})\) be an LD\((n,m,K,\lambda)\). Let \( \mathcal{A}_i = (B_i | i \in I) \). Let us define its incidence relation, for \( x \in X \) and \( i \in I \), by

\[
\rho(x,B_i) = \begin{cases} 
1 & \text{if } x \in B_i, \\
0 & \text{if } x \notin B_i.
\end{cases}
\]

For any 2-set \((x,y) \subseteq X\) such that \( x \) and \( y \) are not in a vertical or horizontal group of this LD, we have, by the definition of an LD, that \( \lambda = \sum_{i \in I} \rho(x,B_i) \rho(y,B_i) \). Thus,

\[
\lambda n(n - 1)m(m - 1) = \sum_{i \in I} \sum_{j \in I} \rho(x,B_i) \rho(y,B_j)
\]

where the first sum is over all ordered pairs \((x,y)\) such that \( x \) and \( y \) belong to different vertical groups as well as different horizontal groups. Interchanging the order of summation, we get
\[ \lambda(n - 1)m(m - 1) = \sum_{i \in I} \sum_{x, y \in X} \rho(x, B_i) \rho(y, B_i) \]

But for every \( i \in I \), the inner sum is \(|B_i|(|B_i| - 1) \equiv 0 \pmod{\beta(K)}\).

Hence,

\[ \lambda(n - 1)m(m - 1) \equiv 0 \pmod{\beta(K)} . \]

Let \( x_o \in X \) be any fixed element. Let \( y \in X \) such that \( x_o \neq y \) and they are in distinct vertical and horizontal groups, then we have, by the definition of an LD, that

\[ \lambda = \sum_{i \in I} \rho(x_o, B_i) \rho(y, B_i) . \]

Thus,

\[ \lambda(n - 1)(m - 1) = \sum_{i \in I} \sum_{y \in X-{x_o}} \rho(x_o, B_i) \rho(y, B_i) . \]

where the first sum is over all points \( y \) such that \( y \neq x_o \), and \( y \) and \( x_o \) belong to different vertical groups as well as different horizontal groups. Interchanging the order of summation, we get

\[ \lambda(n - 1)(m - 1) = \sum_{i \in I} \rho(x_o, B_i) \sum_{y \in X-{x_o}} \rho(y, B_i) . \]

But if \( \rho(x_o, B_i) \neq 0 \), then the inner sum is \(|B_i| - 1 \equiv 0 \pmod{\alpha(K)}\).

Hence,

\[ \lambda(n - 1)(m - 1) \equiv 0 \pmod{\alpha(K)} . \]

Similarly, we have
Proposition 1.36'. Let $n, \lambda \in \mathbb{N}$ and $K \subseteq \mathbb{N}$. If 
$m \in NVG[n, K, \lambda]$, then

$$\lambda n(n - 1)m(m - 1) \equiv 0 \pmod{\beta(K)}, \quad \text{and} \quad (1.11)$$

$$\lambda(n - 1)(m - 1) \equiv 0 \pmod{\alpha(K)} . \quad (1.12)$$

One would naturally ask whether or not (1.9) and (1.10) are 
sufficient for $n \in NHG[m, K, \lambda]$. ((1.11) and (1.12) are sufficient 
for $m \in NVG[n, K, \lambda]$.) One of our main results is that (1.9) and 
(1.10) are 'asymptotically sufficient' for $n \in NHG[m, K, \lambda]$ if $m$ 
is big enough. Similar results for $NVG[m, K, \lambda]$ also hold. As 
we observed before that $n \in NHG[m, K, \lambda]$ iff $m \in NVG[n, K, \lambda]$, we 
shall restrict our attention to $NHG[m, K, \lambda]$. All the results that 
we will get for $NHG[m, K, \lambda]$ will have similar statements for 
$NVG[n, K, \lambda]$.

As a conclusion of this section, we include a 'composition' 
theorem for LD's.

Proposition 1.37. Let $s, m, n, \lambda, \lambda' \in \mathbb{N}$ and $K \subseteq \mathbb{N}, J \subseteq \mathbb{N}$. If 
$n \in NHG[m, J, \lambda'] \cap NHG[s, K, \lambda]$ and $J \subseteq NG[s, K, \lambda]$, then 
n \in NHG[ms, K, \lambda \lambda'] .

Proof: Let $(X, V, H, \mathcal{A})$ be an LD($n, m, J, \lambda'$) where 
$\gamma = \{V_1, \ldots, V_m\}, H = \{H_1, H_2, \ldots, H_n\}$, and $\mathcal{A} = \{B_i \mid i \in I\}$. 
Let $Y_x$ be a set of $s$ elements for every $x \in X$ such that 
$Y_x \cap Y_y = \emptyset$ for all $x, y \in X$ and $x \neq y$. Let $H_i^* = \bigcup_{x \in H_i} Y_x$ for
i ∈ I_n and \( \mathcal{V}^* = \{ \mathcal{V}_i^* | i \in I_n \} \). For every \( i \in I_m \),
\[ |V_i| = n \in \text{NG}[s, K, \lambda] \]. Let \( (\bigcup_{x \in V_i} \mathcal{Y}_x, \mathcal{V}_i, \mathcal{H}_i, \mathcal{G}_i) \) be an LD \((n, s, K, \lambda)\). Without loss of generality, we may assume
\[ \mathcal{H}_i = \{ y_x | x \in V_i \} \]. Let \( \mathcal{V}^* = \bigcup_{i \in I_m} \mathcal{V}_i \) and \( \mathcal{A}_i = (B_{ij} | j \in J_i) \)
for some indexing set \( J_i \). For every \( i \in I, |B_i| \in \text{NG}[s, K, \lambda] \).
Let \( (\bigcup_{x \in B_i} \mathcal{Y}_x, \mathcal{J}_i, \mathcal{A}_i) \) be such a GDD with \( \mathcal{J}_i = \{ y_x | x \in B_i \} \) and \( x \in B_i \)
\[ \mathcal{A}_i = (B_{ij} | j \in L_i) \] for some indexing set \( L_i \). Let \[ \mathcal{H}^* = \Sigma_{i \in I} \mathcal{H}_i + \Sigma_{i=1}^m \lambda' \mathcal{A}_i \]. We claim that \( (\bigcup_{x \in X} \mathcal{Y}_x, \mathcal{V}^*, \mathcal{H}^*, \mathcal{A}^*) \) is an LD \((n, m, s, K, \lambda, \lambda')\).

We need only show that any 2-set of \( X^* = \bigcup_{x \in X} \mathcal{Y}_x \), not contained in a vertical or horizontal group, is contained in exactly \( \lambda \lambda' \) blocks of \( \mathcal{A}^* \). Let \( \{ a, b \} \subseteq X \) be any 2-set not contained in a vertical or horizontal group. Then there are \( x \) and \( y \) of \( X \) such that they are not in a horizontal group of \( \mathcal{H} \) and \( a \in \mathcal{Y}_x \), \( b \in \mathcal{Y}_y \). If \( x \) and \( y \) are in some vertical group \( V_i \) of \( \mathcal{V} \), then \( \{ a, b \} \) is contained in exactly \( \lambda \) blocks of \( (\bigcup_{x \in V_i} \mathcal{Y}_x, \mathcal{V}_i, \mathcal{H}_i, \mathcal{G}_i) \) since \( \mathcal{V}_i \subseteq \mathcal{V}^* \) and \( \{ a, b \} \) are not contained in a vertical group of \( \mathcal{V} \). Hence \( \{ a, b \} \) is contained in exactly \( \lambda \lambda' \) blocks of \( \mathcal{A}^* \). Now if \( x \) and \( y \) are not contained in any vertical group of \( \mathcal{V} \), then \( x \) and \( y \) are contained in exactly \( \lambda' \) blocks of \( \mathcal{A} \), say \( B_1, B_2, \ldots, B_{\lambda'} \). For each of these blocks,
\{(a, b) \subseteq \bigcup_{x \in B_1} Y_x \text{ and } (a, b) \text{ is not in any group of } J_i \text{ for } i \in I_{\lambda'}\}. \text{ Hence } (a, b) \text{ is contained in exactly } \lambda \text{ blocks of } \mathcal{A}_i'. \text{ Thus it is contained in exactly } \lambda \lambda' \text{ blocks of } \mathcal{A}^*, \text{ as claimed.}

We have the similar result by replacing NHG with NVG in Proposition 1.37.
CHAPTER II

GDD'S AND \((m,K,d)\)-PATTERNS

§2.1 Necessary Conditions. For ease of description, we shall discuss GDD's with index of pairwise balance \(\lambda = 1\) in this chapter and the first part of Chapter III. We shall, as mentioned in Chapter I, denote it by GD\((n,m,K)\). Furthermore, we shall deal only with the case when the family of blocks is in fact a class of blocks. Thus, a GD\((n,m,K)\) is a triple \((X,\mathcal{A},\mathcal{B})\) where \(\mathcal{B}\) is a parallel class on \(X\), \(|B| \in K\) for every \(B \in \mathcal{A}\), and, for every 2-set \((x,y) \subseteq X\) not contained in a group of \(\mathcal{B}\), it is contained in a unique block \(B\) of \(\mathcal{A}\). As we mentioned in Chapter I, we assume that \(k \geq 3\) for every \(k \in K\). For notational convenience, we define the function \(e: \mathbb{Z} \to \mathbb{Z}\) by

\[
e(x) = \begin{cases} 
2x & \text{if } x \text{ is odd}, \\
x & \text{if } x \text{ is even}.
\end{cases}
\]

Let \(K \subseteq \mathbb{N}\) be given. Recalling that \(\beta(K) = \gcd(k(k-1) \mid k \in K}\) and \(\alpha(K) = \gcd(k-1 \mid k \in K}\), define
Then we have

Lemma 2.1. Let $K \subseteq \mathbb{N}$ be given. Then $(\alpha(K), \gamma(K)) = 1$.

Proof: If $\alpha(K) = 0$, the assertion is clear. Assume that $\alpha(K) \neq 0$. Let $d = (\alpha(K), \gamma(K))$. Now $\beta(K) = \alpha(K) \cdot \gamma(K) | k(k - 1)$ for every $k \in K$. Thus $d \cdot \alpha(K) | k(k - 1)$ for every $k \in K$. But $d | \alpha(K)$ and $d | k - 1$ for every $k \in K$, i.e. $(k, \alpha(K)) = 1$ and $(d, k) = 1$ for every $k \in K$. Hence $d \cdot \alpha(K) | k - 1$ for every $k \in K$, i.e. $d \cdot \alpha(K) | \alpha(K)$. Hence $d = \pm 1$.

We shall deal primarily with the sets $\text{NG}[m, K]$'s. We recall Proposition 1.24 and obtain that if $n \in \text{NG}[m, K]$, then

$$n(n - 1)m^2 \equiv 0 \pmod{\beta(K)}, \quad \text{and} \quad (2.1)$$

$$(n - 1)m \equiv 0 \pmod{\alpha(K)} \quad (2.2)$$

By Corollary 1.21, we know that $\text{NG}[m, K]$ is a closed set with respect to the closure operation $B$. In view of Theorem 1.10, we first obtain the following proposition.

Proposition 2.2. Let $m \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Then (2.1) and (2.2) are equivalent to the relations
\[ n(n - 1) \equiv 0 \pmod{\beta(m,K)}, \text{ and} \] (2.3)

\[ n - 1 \equiv 0 \pmod{\alpha(m,K)}, \] (2.4)

where

\[ \alpha(m,K) = \frac{\alpha(K)}{(m,\alpha(K))}. \] (2.5)

and

\[ \beta(m,K) = \varepsilon \left( \frac{\beta(K)}{(m^2,\gamma(K))(m,\alpha(K))} \right). \] (2.6)

**Proof:** Clearly, \((n - 1)m \equiv 0 \pmod{\alpha(K)}\) is equivalent to \(n \equiv 1 \pmod{\alpha(m,K)}\). Now assume (2.1) and (2.2). It remains to exhibit (2.3). But (2.1) implies that \(n(n - 1)m^2 \equiv 0 \pmod{\gamma(K)}\) since \(\beta(K) = \alpha(K) \cdot \gamma(K)\). Hence,

\[ n(n - 1) \equiv 0 \pmod{\frac{\gamma(K)}{(m^2,\gamma(K))}}. \]

Since \((\alpha(K),\gamma(K)) = 1\), \(\left(\frac{\alpha(K)}{(m,\alpha(K))}, \frac{\gamma(K)}{(m^2,\gamma(K))}\right) = 1\). Thus,

\[ n(n - 1) \equiv 0 \pmod{\frac{\beta(K)}{(m^2,\gamma(K))(m,\alpha(K))}}, \]

since \(\frac{\alpha(K)}{(m,\alpha(K))} \mid n - 1\). Now \(n(n - 1)\) is even. Therefore,

\[ n(n - 1) \equiv 0 \pmod{\beta(m,K)}. \]
Now let us assume (2.3) and (2.4). It remains to exhibit (2.1). (2.3) implies that

\[
\beta(K) \cdot m^2 | n(n - 1)m^2.
\]

Now \((m^2, \gamma(K))\) and \((m, \alpha(K))\) are relatively prime by Proposition 2.1, and both divide \(m^2\). Hence, we have

\[
\beta(K) \cdot \frac{m^2}{(m^2, \gamma(K))(m, \alpha(K))} | n(n - 1)m^2.
\]

Thus, \(n(n - 1)m^2 \equiv 0 \pmod{\beta(K)}\), as desired.

§2.2 Method of Differences. In [1], R. C. Bose developed a number of methods for direct construction of BIBD's, one of which (the method of difference) arises from investigating the structure of a BIBD with respect to a given group of automorphisms. By an automorphism of a design \((X, \mathcal{A})\), we mean a permutation \(\sigma\) on \(X\) such that for all subsets \(A \subseteq X\), the multiplicity of \(A^\sigma\) in \(\mathcal{A}\) is the same as that of \(A\) in \(\mathcal{A}\) where \(A^\sigma\) is defined to be \(A^\sigma = \{x^\sigma \mid x \in A\}\). We will also apply this method of differences to construct a certain class of GDD's.

Let \(G\) be a finite additive abelian group. For a subset \(B \subseteq G\), the list of differences from \(B\) is defined to be \(\Delta B = (a - b \mid a, b \in B, a \neq b)\). And if \(G = (B_i \mid i \in I)\) is a
family of subsets of $G$, we define $\Delta B = \sum_{i \in I} \Delta B_i$. Given a subset $B \subseteq G$, define, for any $g \in G$, $B + g = \{b + g \mid b \in B\}$. Let $x, y \in G$ be two distinct elements and $B \subseteq G$ be given. Define $T = \{g \in G \mid (x, y) \in B + g\}$ and $D = \{(a, b) \mid a, b \in B; a - b = x - y\}$. Then the mapping $\varphi: T \to D$ defined by $\varphi(g) = (x - g, y - g)$ is bijective. Thus, the number of $g \in G$ such that $(x, y) \in B + g$ is the number of times $x - y$ occurs in the list $\Delta B$.

Let $m \in \mathbb{N}$ be a given integer and $q$ be a prime power. Let $X = I_m \times \mathbb{F}(q)$. Write $G_u = I_m \times \{u\}$ for every $u \in \mathbb{F}(q)$. Let $\mathcal{S} = \{G_u \mid u \in \mathbb{F}(q)\}$. Let $B \subseteq X$ be a given $k$-subset, say

$$B = \{(\ell_1, b_1), (\ell_2, b_2), \ldots, (\ell_k, b_k)\},$$

where $b_i \in \mathbb{F}(q)$, $\ell_i \in I_m$ for $i \in I_k$. For $a, c \in \mathbb{F}(q)$, define the set

$$aB + c = \{(\ell_1, ab_1 + c), (\ell_2, ab_2 + c), \ldots, (\ell_k, ab_k + c)\}.$$

For every $\ell \in I_m$, let $\Delta_p(B, \ell)$ denote the list of elements of $\mathbb{F}(q)$ which contain an entry $u - v$ for every ordered pair $((\ell, u), (\ell, v))$ of distinct elements of $B$. For every $1 \leq \ell_1 < \ell_2 \leq m$, let $\Delta_r(B, (\ell_1, \ell_2))$ denote the list of elements of $\mathbb{F}(q)$ which contain an entry $u - v$ for every ordered pair $((\ell_1, v), (\ell_2, u))$ of elements of $B$. If $\mathcal{B} = \{B_1, B_2, \ldots, B_t\}$, let us define $\Delta_p(\mathcal{B}, \ell) = \sum_{i=1}^{t} \Delta_p(B_i, \ell)$ for every $\ell \in I_m$. and
\[ \Delta_M(\emptyset, (l_1, l_2)) = \sum_{i=1}^{t} \Delta_M(B_i, (l_1, l_2)) \] for every \( 1 \leq l_1 < l_2 \leq m \). With this terminology in mind, we observe the following very important fact.

**Proposition 2.3.** Let \( K \subseteq \mathbb{N} \) be a given subset. Let
\[ \emptyset = \{B_1, B_2, \ldots, B_t\} \] be a family of given subsets of \( X \) such that \( |B_i| \in K \) for every \( i \in I_t \) and \( |B_i \cap G_u| \leq 1 \) for every \( u \in GF(q) \) and every \( i \in I_t \). The triple
\[ (X, \emptyset, \bigcup_{i=1}^{t} (B_i + c \mid c \in GF(q))) \] is a \( GD(q,m,K) \) iff

(i) for every \( \ell \in I_m \), \( \Delta_p(\emptyset, \ell) = GF(q)^* = GF(q) - \{0\} \)
(i.e. \( \Delta_p(\emptyset, \ell) \) contains every non-zero element of \( GF(q) \) exactly once).

(ii) for every \( 1 \leq l_1 < l_2 \leq m \), \( \Delta_M(\emptyset, (l_1, l_2)) = GF(q)^* \).

**Proof:** Necessity is clear. To prove sufficiency, let \( (l_2, a) \) and \( (l_1, b) \) be two distinct elements of \( X \), not contained in a same group of \( \emptyset \), i.e. \( a \neq b \). Then \( a - b \in GF(q)^* \). If \( l_1 = l_2 = \ell \), then, by (i), there is a unique \( i_0 \in I_t \) such that \( a - b \in \Delta_p(B_{i_0}, \ell) \). Then there are exactly two distinct \( u \) and \( v \) of \( GF(q) \) such that \( (\ell, u) \) and \( (\ell, v) \) are contained in \( B_{i_0} \) and \( u - v = a - b \). By the argument made at the beginning of this section, the number of \( c \in GF(q) \) such that \( ((\ell, a), (\ell, b)) \subseteq B_{i_0} + c \) is the number of times that \( a - b \) occurs in the list \( \Delta_p(B_{i_0}, \ell) \). By (i) again, there is a unique \( c_0 \in GF(q) \) such that \( ((\ell, a), (\ell, b)) \subseteq B_{i_0} + c_0 \).
If \( \ell_1 < \ell_2 \), then by (ii), there is a unique \( i_1 \in I_t \) such that \( \Delta_M(B_{i_1}, (\ell_1, \ell_2)) \) contains \( a - b \). Then there are exactly two distinct elements \( u \) and \( v \) of \( \text{GF}(q) \) such that 
\[
\{(\ell_1, v), (\ell_2, u)\} \subseteq B_{i_1} \quad \text{and} \quad u - v = a - b.
\]
By the same argument as before, there is a unique \( c_1 \in \text{GF}(q) \) such that 
\[
\{(\ell_1, a), (\ell_2, b)\} \subseteq B_{i_1} + c_1.
\]

**Remark.** We will get a GD\((n, m, K, \lambda)\) if the conditions (i) and (ii) are replaced by \( \Delta_P(\theta, \lambda) = \lambda \cdot (\text{GF}(q))^\ast \) and 
\[
\Delta_M(\theta, (\ell_1, \ell_2)) = \lambda \cdot (\text{GF}(q))^\ast
\]
respectively. The above proposition is still true if we replace the set \( I_m \) by any \( m \)-set \( M \). The modifications to the statement and its proof are easily seen.

§2.3 The Existence of GD\((n, m, K)\). We shall devote the rest of this chapter and part of Chapter III to proving one of the main results, namely,

**Theorem 2.4.** Let \( m \in \mathbb{N} \) be a given integer and \( K \subseteq \mathbb{N} \) be a given subset. Then there exists a constant \( N = N(m, K) \) such that, for all \( n \geq N \) satisfying (2.1) and (2.2), 
\[
n \in NG[m, K].
\]

Recalling Proposition 2.2, we have that, given \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \), if \( n \in NG[m, K] \), then
n(n - 1) \equiv 0 \pmod{\beta(m,K)}, \quad \text{and}
\n\n- 1 \equiv 0 \pmod{\alpha(m,K)},

where \( \alpha(m,K) = \frac{\alpha(k)}{(m,\alpha(k))} \) and \( \beta(m,K) = \epsilon \left( \frac{\beta(k)}{(m^2,\gamma(k))(m,\alpha(k))} \right) \).

We know, by Corollary 1.21, that \( NG[m,K] \) is a closed set. In view of Theorem 1.10, we have

**Theorem 2.5.** Let \( m \in \mathbb{N} \) be a given integer and \( K \subseteq \mathbb{N} \) be a given subset. If \( \beta(m,K) = \beta(NG[m,K]) \) and \( \alpha(m,K) = \alpha(NG[m,K]) \), then there exists a constant \( N = N(m,K) \) such that, for all \( n \geq N \) satisfying (2.1) and (2.2), we have \( n \in NG[m,K] \).

**Proof:** If \( \beta(m,K) = \beta(NG[m,K]) \) and \( \alpha(m,K) = \alpha(NG[m,K]) \), then, since \( NG[m,K] \) is a closed set, we have by Theorem 1.10 that \( NG[m,K] \) contains all sufficiently large \( n \in \mathbb{N} \) satisfying (2.3) and (2.4). By Proposition 2.2, (2.3) and (2.4) are equivalent to (2.1) and (2.2). Hence there exists a constant \( N = N(m,K) \) such that, for all \( n \geq N \) satisfying (2.1) and (2.2), we have \( n \in NG[m,K] \).

As we mentioned in Chapter I, a \( GD(n,1,K) \) is actually a PBD. Hence we assume, from now on, that \( m \geq 2 \). Also, remember, as we stated in §2.1, that \( k \geq 3 \) for any \( k \in K \). In view of Theorem 2.5, it suffices to establish that \( \beta(m,K) = \beta(NG[m,K]) \) and \( \alpha(m,K) = \alpha(NG[m,K]) \) in order to prove the main result,
Theorem 2.4. The rest of this chapter is devoted to computing $\beta(NG[m,K])$. Chapter III is devoted to establishing the fact that $\alpha(m,K) = \alpha(NG[m,K])$.

If $K = \{k\}$, we shall write $\beta(m,k)$ instead of $\beta(m,\{k\})$ and $\alpha(m,k)$ instead of $\alpha(m,\{k\})$.

§2.4 (m,K,d) - Pattern. In order to establish the fact that $\beta(m,K) = \beta(NG[m,K])$ for a finite set $K \subseteq N$, we require the existence of a certain class of GDD's. The constructions are effected with the use of finite field and Theorem 1.11.

Before we construct this class of GDD's, we introduce a new kind of combinatorial configuration which will be used to help us construct GDD's. Let $d \in N$ be a given integer. Let $m \geq 2$ be a given positive integer. Let $K \subseteq N$ be a given subset (finite or infinite). Let $X = \{x_1, x_2, \ldots, x_m\}$ be a set of $m$ different symbols. Consider the polynomial ring $\mathbb{Z}[x_1, x_2, \ldots, x_m]$.

Define the set

$$S_K(X) = \{ \sum_{i=1}^{m} a_i x_i \mid a_i \in \mathbb{N}_0, \sum_{i=1}^{m} a_i \in K \} \subseteq \mathbb{Z}[x_1, x_2, \ldots, x_m].$$

We shall write $S_K(X)$ instead of $S_{\{K\}}(X)$. It is easy to see that $S_K(X) = \bigcup_{k \in K} S_k(X)$. For any $f \in S_K(X)$, we shall use
\( f(x_s) \) to denote the coefficient of \( x_s \) in \( f \), for any \( s \in I_m \).

**Definition.** An \((m,K,d)\)-pattern is a pair \((X,L)\) where

(i) \( X = \{x_1, x_2, \ldots, x_m\} \) is a finite set of elements,

(ii) \( L \) is a family (list) of elements of \( F_K(X) \), say
    \[ L = (f_i | i \in I) \]
    for some indexing set \( I \),

(iii) for any 2-set \( \{s,t\} \subseteq I_m \), \( \Sigma_{i \in I} f_i(x_s)f_i(x_t) = d \),

(iv) for any \( s \in I_m \), \( \Sigma_{i \in I} f_i(x_s)(f_i(x_s) - 1) = d \).

The elements of \( X \) will be called **points** and the entries of \( L \) will be called **blocks**. We shall write \((m,k,d)\)-pattern instead of \((m,\{k\},d)\)-pattern. Clearly, \( d \) must be an even integer.

For convenience, we shall view \( f \in F_k(X) \) as a \( k \)-tuple in \( X^k = X \times X \times \ldots \times X \). In fact, let us write

\[
\begin{align*}
f(x_s)x_s + f(x_t)x_t + \ldots + f(x_w)x_w,
\end{align*}
\]

where we omit the terms \( x_i \) if \( f(x_i) = 0 \), \( s \) is the smallest integer in \( I_m \) such that \( f(x_s) \neq 0 \), and \( w \) is the biggest integer in \( I_m \) such that \( f(x_w) \neq 0 \). Then we may view \( f \) as a \( k \)-tuple in \( X^k \), namely,

\[
\begin{align*}
\underbrace{(x_s,x_s, \ldots, x_s, x_t, x_t, \ldots, x_t, \ldots, x_w, x_w, \ldots, x_w)}_{f(x_s) \text{ times }} \underbrace{f(x_t) \text{ times }}_{f(x_t) \text{ times }} \underbrace{f(x_w) \text{ times}}_{f(x_w) \text{ times }}
\end{align*}
\]

where \( s < t < \ldots < w \)

Now, since \( |X| = m \), we may even regard \( f \) as a \( k \)-tuple in \( I_m^k \), i.e.
For notational convenience, denote the \( k \)-tuple above by 
\[
(y^1_1, y^2_1, \ldots, y^k_1), \quad \text{where} \quad s = y^1_1 = y^2_1 = \ldots = y^k_1,
\]
\[
t = y^t_1 + 1 = \ldots = y^t_1 + f(x^t_1) + f(x^t_1), \quad \ldots, \quad w = y^w_k + f(x^w_k) + 1 = \ldots = y^w_k.
\]

Define the set, for \( k, m \in \mathbb{N} \),
\[
I^f_k(m) = \{(b^1, b^2, \ldots, b^k) \mid b^s \in \mathbb{I}_m \text{ for } s \in I_k, \quad b^s \leq b^{s+1} \text{ for } s \in I_k-1\}.
\]

The mapping \( \varphi: I^f_k(X) \rightarrow I^f_k(m) \) defined by
\[
\varphi(f) = (y^1_1, y^2_1, \ldots, y^k_1)
\]
is a one-to-one correspondence. Let \( I^f_k(m) = \bigcup_{k \in \mathbb{K}} I^f_k(m) \).

For any \( T = (b^1_t, b^2_t, \ldots, b^k_t) \in I^f_k(m) \), let \( a^T_s \) denote the number of indices \( j \in I_k \) such that \( b^j_s = s \) for any \( s \in \mathbb{I}_m \).

Define the subset \( M^f_T(s, t) \) of \( I^f_k \times I^f_k \), for any \( s, t \in \mathbb{I}_m \),
\( s \neq t \),
\[
M^f_T(s, t) = \{(u, v) \mid 1 \leq u, v \leq k, u \neq v, b^u_s = s, b^v_t = t\}.
\]

Then \( |M^f_T(s, t)| = a^T_s a^T_t = |M^f_T(t, s)| \). Moreover, for \( 1 \leq s < t \leq m \),
we have
\[
M^f_T(s, t) = \{(u, v) \mid 1 \leq u < v \leq k, b^u_s = s, b^v_t = t\}.
\]
For any $s \in I_m$, define the subset $M_T(s,s)$ of $I_k \times I_k$ by

$$M_T(s,s) = \{(u,v) | 1 \leq u < v \leq k, b_u = b_v = s\}.$$  

Then $|M_T(s,s)| = a_s^T(a_s^T - 1)/2$.

Let $L = (T_i | i \in I)$ be a family of elements of $L_K(m)$. Then, for every $i \in I$, there is a unique $k_i \in K$ such that $T_i \in L_{k_i}(m)$. We shall write $T_i = (b^i_1, b^i_2, \ldots, b^i_{k_i})$. We shall write $M_i(s,t)$ instead of $M_T^i(s,t)$, namely,

$$M_i(s,t) = \{(u,v) | 1 \leq u < v < k_i, u \neq v, b^i_u = s, b^i_v = t\},$$

for every $(s,t) \in I_m$, and $M_i(s,s)$ instead of $M_T^i(s,s)$, namely,

$$M_i(s,s) = \{(u,v) | 1 \leq u < v \leq k_i, b^i_u = b^i_v = s\}$$

for every $s \in I_m$.

Furthermore, write $a^i_s$ instead of $a^T_i$ for every $s \in I_m$ and every $i \in I$. With this terminology in mind and the aid of the one-to-one correspondence $\varphi$, we have an equivalent definition for an $(m, K, d)$-pattern.

**Definition.** Let $d, m \in W$ and $K \subseteq W$ be given. An $(m, K, d)$-pattern is a pair $(I_m, L)$ where

1. $L$ is a family of elements of $L_K(m)$, say
$L = (T_i \mid i \in I)$ for some indexing set $I$,

(ii) for every 2-set $\{s, t\} \subseteq I_m$ such that $s < t$,

$$\sum_{i \in I} |M_i(s, t)| = d,$$

(iii) for every $s \in I_m$,

$$\sum_{i \in I} |M_i(s, s)| = \frac{d}{2}.$$

From now on, we shall use these two definitions interchangeably.

For notational convenience, let us write $m_i(s, t)$ instead of $|M_i(s, t)|$ and $m_i(s, s)$ instead of $|M_i(s, s)|$. Now let us consider some examples of patterns. However, for ease of description, we only discuss the case when $K = \{k\}$.

**Example 1.** $m = 2, k = 4, d = 6$.

Let $L = \{(1,1,1,2), (1,2,2,2)\} \subseteq I_4(2)$. Put $T_1 = (1,1,1,2)$ and $T_2 = (1,2,2,2)$. Thus, $m_1(1,1) = 3 = m_2(2,2)$, $m_1(1,2) = 3 = m_2(2,1)$, and $m_1(2,2) = 0 = m_2(1,1)$. Hence,

$$\sum_{i=1}^{2} m_i(1,2) = 6 \quad \text{and} \quad \sum_{i=1}^{2} m_i(1,1) = 3 = \sum_{i=1}^{2} m_i(2,2),$$

i.e. $(I_2, L)$ is a $(2,4,6)$-pattern.

**Example 2.** $m = 3, k = 4, d = 4$.

Let $L = \{(1,1,2,2), (2,2,3,3), (1,1,3,3)\} \subseteq I_4(3)$. Put $T_1 = (1,1,2,2), T_2 = (2,2,3,3)$, and $T_3 = (1,1,3,3)$. Thus, $m_1(1,1) = 1 = m_1(2,2) = m_2(2,2) = m_2(3,3) = m_3(1,1) = m_3(3,3)$, $m_1(1,2) = 4 = m_2(2,3) = m_3(1,3)$, and the rest $m_i(s, t) = 0$ for
s, t ∈ I_3 and for i ∈ I_3. Hence, \( \sum_{i=1}^{3} m_i(s, s) = 2 \) for every s ∈ I_3, and \( \sum_{i=1}^{3} m_i(s, t) = 4 \) for any 1 ≤ s < t ≤ 3, i.e. (I_3, L) is a (3, 4, 4)-pattern.

**Example 3.** m = 2, k = 5, d = 20.
Let L = (T_i | i ∈ I_5) be a list of elements of \( I_5(2) \) where

T_1 = (1, 1, 1, 2, 2), T_2 = (1, 1, 2, 2, 2), T_3 = (1, 2, 2, 2, 2), and

T_4 = (1, 1, 1, 1, 2). Thus, \( m_1(1, 1) = 3 \), \( m_1(2, 2) = 1 \), \( m_1(1, 2) = 6 \),

\( m_2(1, 1) = 1 \), \( m_2(2, 2) = 3 \), \( m_3(1, 1) = 0 \), \( m_3(2, 2) = 6 \), \( m_4(1, 1) = 6 \),

\( m_4(2, 2) = 0 \), \( m_4(1, 2) = 6 \), \( m_5(1, 2) = 4 \), \( m_4(1, 2) = 4 \). Hence

\( \sum_{i=1}^{4} m_1(1, 2) = 20 \) and \( \sum_{i=1}^{4} m_1(1, 1) = \sum_{i=1}^{4} m_1(2, 2) = 10 \), i.e.

(I_2, L) is a (2, 5, 20)-pattern.

**Example 4.** m = 5, k = 5, d = 4.
Let L = (T_i | i ∈ I_5) be a list of elements of \( I_5(5) \) where

T_1 = (1, 1, 2, 3, 3), T_2 = (2, 2, 3, 4, 4), T_3 = (3, 3, 4, 5, 5),

T_4 = (1, 1, 4, 4, 5), and T_5 = (1, 2, 2, 5, 5). Thus, \( m_1(1, 1) = 1 = m_1(3, 3) = m_2(2, 2) = m_2(4, 4) = m_3(3, 3) = m_3(5, 5) = m_4(1, 1) = m_4(4, 4) = m_4(5, 5) = m_5(1, 2) = m_5(2, 2) = m_5(4, 5) = m_5(1, 5) = m_5(2, 1) = m_5(2, 3) = m_5(3, 4) = m_5(4, 5) = m_5(1, 5) = m_5(2, 5) = 4 \).

Hence, \( \sum_{i=1}^{5} m_i(j, j) = 2 \) for every j ∈ I_5 and \( \sum_{i=1}^{5} m_i(s, t) = 4 \) for 1 ≤ s < t ≤ 5, i.e. (I_5, L) is a (5, 5, 4)-pattern.
§2.5 GDD's from (m,K,d)-Pattern. In this section, we will show how to get a GD(q,m,K) from a given (m,K,d)-pattern. We start with an example. Recall Example 1 in §2.4, namely, the (2,4,6)-pattern (I₂, L) where \( L = \{(1,1,1,2), (1,2,2,2)\} \). Let \( q = 43 \). Then \( q \) is a prime power such that \( q \equiv 1 \pmod{6} \) and \( q^\frac{q-1}{6} \) is odd. It is easy to see that 3 is a primitive root of \( \text{GF}(q) \). For notational convenience, let \( \omega = 3 \). Recall the definition for \( H^6_i \) in §1.2, i.e.

\[
H^6_i = \{\omega^t \mid t \equiv i \pmod{6}\} \text{ for } i = 0, 1, 2, \ldots, 5.
\]

In fact, if we work with \( \mathbb{Z}_{43} \), then we have that

\[
\begin{align*}
H^6_0 &= \{1, 14, 4, 35, 16, 11, 21\}, & H^6_1 &= \{3, 37, 12, 19, 5, 33, 20\}, \\
H^6_2 &= \{9, 25, 36, 14, 15, 13, 17\}, & H^6_3 &= \{27, 32, 42, 2, 39, 8\}, \\
H^6_4 &= \{38, 10, 23, 40, 6, 31, 24\}, & H^6_5 &= \{28, 30, 26, 34, 18, 7, 29\}.
\end{align*}
\]

Observe that \(-1 \in H^6_3\). Suppose that we could find two 4-tuples of elements of \( \text{GF}(q)\), \((x,y,z,w)\) and \((a,b,c,d)\), such that

(i) the differences \( y - x, z - x, w - x, d - a, d - b, d - c \) form a system of representatives for \( H^6 \),

(ii) the differences \( y - z, z - y, w - z, z - w, w - y \), \( y - w \) form a system of representatives for \( H^6 \),

(iii) the differences \( a - b, b - a, a - c, c - a, b - c, c - b \) form a system of representatives for \( H^6 \),

where \( H^6 = \{H^6_0, H^6_1, \ldots, H^6_5\} \). Let \( B_1 = \{(1,a),(1,b),(1,c),(2,d)\} \)
$B_2 = \{(1,x),(2,y),(2,x),(2,w)\}$. Define the sets

$$B_{1,i} = \omega^{6i}B_1 = \{(1,\omega^{6i}a),(1,\omega^{6i}b),(1,\omega^{6i}c),(2,\omega^{6i}d)\},$$

$$i = 0, 1, 2, \ldots, 6.$$ 

and

$$B_{2,i} = \omega^{6i}B_2 = \{(1,\omega^{6i}x),(2,\omega^{6i}y),(2,\omega^{6i}z),(2,\omega^{6i}w)\},$$

$$i = 0, 1, 2, \ldots, 6.$$ 

Then, for any $\ell \in I_2$, the list of differences $u - v$, where $(\ell,u)$ and $(\ell,v)$ are contained in some $B_{1,i}$ or $B_{2,i}$, contains every nonzero element of $GF(q)$ exactly once, because of (ii) and (iii) above, and the fact that $H^6 = \{\omega^{6i} \mid i = 0, 1, 2, \ldots, 6\}$.

And, the list of differences $v - u$, where $(1,u)$ and $(2,v)$ are contained in some $B_{1,i}$ or $B_{2,i}$, contains every nonzero element exactly once, because of (i) above. Now, by Proposition 2.3, $(I_2 \times GF(q), \mathcal{A})$ is a GD($q,2,4$) where $\mathcal{A} = [I_2 \times \{u\} \mid u \in GF(q)]$ and

$$\mathcal{A} = \bigcup_{i=0}^{6} (B_{1,i} + c \mid c \in GF(q)) \cup \bigcup_{i=0}^{6} (B_{2,i} + c \mid c \in GF(q)).$$

It remains to exhibit two 4-tuples, $(x,y,z,w)$ and $(a,b,c,d)$, of elements of $GF(q)$, satisfying (i), (ii), and (iii) above. By an easy calculation, we see that $(1,3,39,11)$ and $(11,1,3,39)$
satisfy (i), (ii) and (iii) above for \((a,b,c,d)\) and \((x,y,z,w)\), respectively.

Let \(K \subseteq \mathbb{N}\) be a finite set. Let \((I_m, L)\) be an \((m,K,d)\)-pattern where \(L = (T_i | i \in I)\) for some indexing set \(I\). By definition,

\[
\sum_{i \in I} m_i(s,t) = d, \text{ for every } 1 \leq s < t \leq m.
\]

Let \(q \in \mathbb{N}\) be a prime power such that \(q \equiv 1 \pmod{d}\) and \(\frac{q-1}{d}\) is odd. Hence, we can partition \(\mathbb{N}^d\), the class of cosets of \(\text{GF}(q)^*\) modulo \(d\)-th powers, into \(\mathbb{N}^d = \bigcup_{i \in I} H_i(s,t)\) such that \(|H_i(s,t)| = m_i(s,t)\) for every \(i \in I\), i.e. there exists a one-to-one correspondence \(g_{s,t,i} : M_i(s,t) \to H_i(s,t)\) for every \(i \in I\) and every \(1 \leq s < t \leq m\). Now, we also have that

\[
\sum_{i \in I} m_i(s,s) = \frac{d}{2}, \text{ for every } s \in I_m.
\]

Define \(\mathbb{N}_{1/2}^d = \{H_j^d | j = 0, 1, 2, \ldots, \frac{d}{2} - 1\}\). Hence, we can also partition \(\mathbb{N}_{1/2}^d\) into \(\mathbb{N}_{1/2}^d = \bigcup_{i \in I} H_i(s,s)\) such that \(|H_i(s,s)| = m_i(s,s)\) for every \(i \in I\), i.e. there exists a one-to-one correspondence \(g_{s,s,i} : M_i(s,s) \to H_i(s,s)\) for every \(s \in I_m\) and every \(i \in I\).

Now, for every \(i \in I\), there is a unique \(k_i\) of \(K\) such that \(T_i \in L_{k_i}(m)\). Consider the set
Recall that, for every \( s \in \mathbb{I}_m \), \( a_s^i \) is the number of indices \( j \in I_{k_i} \) such that \( y_j^i = s \) where \( T_i = (y_1^i, y_2^i, \ldots, y_{k_i}^i) \). Then \( P_{k_i} \) can be partitioned as

\[
( \bigcup_{s=1}^{m} M_i(s,s)) \cup \bigcup_{1 \leq s < t \leq m} M_i(s,t))
\]

(This can be verified very easily.) Hence, we can define, for every \( i \in I \), a choice function \( C_i : P_{k_i} \rightarrow \mathbb{N}_d \) as follows:

\[
C_i(u,v) = \begin{cases} 
\hat{g}_{s,t,i}(u,v) & \text{if } (u,v) \in M_i(s,t) \text{ for some } 1 \leq s < t \leq m, \\
\hat{g}_{s,s,i}(u,v) & \text{if } (u,v) \in M_i(s,s) \text{ for some } s \in \mathbb{I}_m.
\end{cases}
\]

Now suppose \( q > d \). By Theorem 1.11, there exists, for every \( i \in I \), a \( k_i \)-tuple \( (z_1^i, z_2^i, \ldots, z_{k_i}^i) \) of elements of GF(q) such that \( z_v^i - z_u^i \in C_i(u,v) \) for any \( 1 \leq u < v \leq k_i \).

For every \( i \in I \), let us define the set

\[
B_i = \{(y_1^i, z_1^i), (y_2^i, z_2^i), \ldots, (y_{k_i}^i, z_{k_i}^i)\}.
\]

Let \( s, t \in \mathbb{I}_m \) be any two distinct elements such that \( s < t \). Recall the partition \( \mathbb{I}_m = \bigcup_{i \in I} H_i(s,t) \) such that \( |H_i(s,t)| = m_i(s,t) \).
and the one-to-one correspondence \( g_{s,t,i} : M_i(s,t) \rightarrow H_i(s,t) \) for every \( i \in I \). Hence, the list of differences \( z^i_v - z^i_u \), for \( i \in I \), such that \( y^i_u = s \) and \( y^i_v = t \), forms a system of representatives for \( H^d \). Let \( s \in I_m \) be any element. Recall the partition \( H^d_{1/2} = \bigcup_{i \in I} H_i(s,s) \) such that \( |H_i(s,s)| = m_i(s,s) \)

and the one-to-one correspondence \( g_{s,s,i} : M_i(s,s) \rightarrow H_i(s,s) \) for every \( i \in I \). Hence the list of differences \( z^i_v - z^i_u \) for \( i \in I \), such that \( u < v \) and \( y^i_u = y^i_v = s \), forms a system of representatives for \( H^d_{1/2} \). But \( \frac{q-1}{d} \) is odd. Hence \( -1 \notin H^d_0 \) and \( -1 \in H^d_{d/2} \).

Therefore, the list of differences \( z^i_v - z^i_u \), for \( i \in I \), \( u \neq v \) such that \( y^i_u = y^i_v = s \), form a system of representatives for \( H^d \).

Now let us consider the sets

\[
B_{i,j} = B_i w^{jd} = \{(y^i_1, z^i_1 w^{jd}), (y^i_2, z^i_2 w^{jd}), \ldots, (y^i_k, z^i_k w^{jd})\} \quad (2.7)
\]

for \( i \in I \) and \( j = 0, 1, 2, \ldots, e-1 \) where \( q-1 = ed \). Since \( H^d_0 = \{1, w, \ldots, w^{(e-1)d}\} \), we have, by Proposition 2.3,

**Theorem 2.6.** Let \( m, d \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be a given finite set.

Suppose that an \((m,K,d)\)-pattern exists, say \((I_m,L)\) where

\( L = (T_i | i \in I) \) for some indexing set \( I \). Let \( q \in \mathbb{N} \) be a prime power such that \( q = d+1 \) (mod \( 2d \)) (i.e. \( q = 1 \) (mod \( d \)) and \( \frac{q-1}{d} \) is odd) and \( q > d^{\max(K)(\max(K) - 1)} \).

Let \( X = I_m \times GF(q) \), \( G_u = I_m \times \{u\} \) for every \( u \in GF(q) \), and \( \mathcal{J} = \{G_u | u \in GF(q)\} \). Define
\[ \mathcal{D} = \bigcup_{i=0}^{\epsilon-1} \bigcup_{i \in I} \{ B_{i,j} + c \mid c \in \text{GF}(q) \} \] where \( B_{i,j} \) is defined by

\[ (2.7) \text{ for } i \in I, j = 0, 1, \ldots, \epsilon - 1, \]

then \((X, \mathcal{J}, \mathcal{D})\) is a GD\((q, m, K)\).

§2.6 Existence of \((m, K, d)\)-Pattern. In this section, we will assume that \(K\) is a set of positive integers. Let \(m, d \in \mathbb{N}\) be given. Let \(X = \{x_1, x_2, \ldots, x_m\}\) be a set of \(m\) symbols.

Consider the set \(L_K(X)\), a subset of the polynomial ring \(\mathbb{Z}[x_1, x_2, \ldots, x_m]\), defined in §2.4. Recall that \(f(x_s)\) denotes the coefficient of \(x_s\) in \(f\) for any \(f \in L_K(X)\) and for any \(s \in I_m\). Let \(f \in L_K(X)\); define the 'pseudo-square of \(f\)' by

\[ f^{(2)} = \sum_{s=1}^{m} f(x_s)(f(x_s) - 1)x_s^2 + \sum_{1 \leq s, t \leq m} f(x_s)f(x_t)x_s x_t. \]

For instance, if \(f = 2x_1 + 3x_2\), then \(f^{(2)} = 2x_1^2 + 6x_1x_2 + 6x_2x_1 + 6x_2^2\). As another example, if \(f = x_1 + x_2\), then

\[ f^{(2)} = x_1x_2 + x_2x_1. \]

First of all, let us examine the necessary conditions for the existence of an \((m, K, d)\)-pattern. Clearly, \(d\) must be an even integer by the definition of an \((m, K, d)\)-pattern. Let \((X, L)\) be an \((m, K, d)\)-pattern where \(L = \{ f_i \mid i \in I \}\) is a family of elements
of $L_K(X)$ for some indexing set $I$. There are exactly $m(m - 1)$ distinct ordered pairs $(x_s, x_t)$ of elements of $X$ with $s \neq t$. Therefore, by definition, we have

$$m(m - 1)d + md = \sum_{1 \leq s, t \leq m} \sum_{i \in I} f_i(x_s)f_i(x_t) +$$

$$\sum_{s=1}^{m} \sum_{i \in I} f_i(x_s)(f(x_s) - 1).$$

So,

$$dm^2 = \sum_{i \in I} [(\sum_{s=1}^{m} f_i(x_s))^2 - \sum_{s=1}^{m} f_i(x_s)].$$

But $\sum_{s=1}^{m} f_i(x_s) \in K$ for every $i \in I$. Hence, we have

$$dm^2 \equiv 0 \pmod{\beta(K)}.$$

Now, let $x_s \in X$ be any fixed element of $X$. Then, again by definition,

$$(m - 1)d + d = \sum_{t \in I} \sum_{i \in I} f_i(x_s)f_i(x_t) +$$

$$\sum_{t \neq s} \sum_{i \in I} f_i(x_s)(f_i(x_s) - 1).$$

So,
A gain, since \( \sum_{i \in I} f_i(x_s) \in K \) for every \( i \in I \), we have
\[
\sum_{i \in I} f_i(x_s) = 0 \pmod{\alpha(K)}.
\]

Hence, we have the following

**Proposition 2.7.** The necessary conditions for the existence of an \((m,K,d)\)-pattern are

\[
\begin{align*}
(i) \quad & d \text{ is even}, \quad (2.8) \\
(ii) \quad & dm^2 \equiv 0 \pmod{\beta(K)}, \quad (2.9) \\
(iii) \quad & dm \equiv 0 \pmod{\alpha(K)}. \quad (2.10)
\end{align*}
\]

Let us reduce the necessary conditions to a condition which will be useful to us. Indeed, we have

**Proposition 2.8.** Let \( m,d \in N \) and \( K \subseteq N \) be given. Then the relations (2.8), (2.9), and (2.10) are equivalent to

\[
d \equiv 0 \pmod{\beta(m,K)}, \quad (2.11)
\]

where, as defined in §2.1, \( \beta(m,K) = \epsilon(\frac{\beta(K)}{(m^2,\gamma(K))(m,\alpha(K))}) \).

**Proof:** Obviously, \( dm \equiv 0 \pmod{\alpha(K)} \) is equivalent to
\[
d = 0 \pmod{\alpha(m, K)} \text{ where } \alpha(m, K) = \frac{\alpha(K)}{(m, \alpha(K))} \text{ as defined in §2.1.}
\]

Now assume (2.8), (2.9), and (2.10). Since \( \beta(K) = \alpha(K)\gamma(K) \), (2.9) implies that \( dm^2 \equiv 0 \pmod{\gamma(K)} \). In turn, it implies that
\[
d \equiv 0 \pmod{\frac{\gamma(K)}{(m^2, \gamma(K))}}.
\]

Since \((\alpha(K), \gamma(K)) = 1\), \( \left( \frac{\alpha(K)}{(m, \alpha(K))}, \frac{\gamma(K)}{(m^2, \gamma(K))} \right) = 1 \). Thus,
\[
d \equiv 0 \pmod{\beta(K)} \pmod{(m^2, \gamma(K))(m, \alpha(K))}.
\]

But (2.8) says that \( d \) is even. Hence,
\[
d \equiv 0 \pmod{\beta(m, K)}.
\]

Next, let us assume (2.11). Clearly, \( d \) must be even since \( \beta(m, K) \) is even. Since \( \alpha(K) \pmod{(m, \alpha(K))} \big| \beta(m, K) \), \( d \equiv 0 \pmod{\frac{\alpha(K)}{(m, \alpha(K))}} \), i.e.
\[
dm = 0 \pmod{\alpha(K)}.
\]

(2.11) implies that
\[
dm^2 = 0 \pmod{\frac{\beta(K)}{(m^2, \gamma(K))(m, \alpha(K))}} \cdot m^2 | dm^2.
\]

Since \((m^2, \gamma(K)) \) and \((m, \alpha(K)) \) are relatively prime, and both divide \( m^2 \), we have
\[ \beta(K) \cdot \frac{m^2}{(m^2, \gamma(K))(m, \alpha(K))} \mid dm^2, \]

i.e.

\[ dm^2 \equiv 0 \pmod{\beta(K)}. \]

One would naturally ask whether (2.8), (2.9), and (2.10) are sufficient for the existence of an \((m, K, d)\)-pattern. It turns out to be 'asymptotically sufficient.' In fact, one of our main results is

**Theorem 2.9.** Let \( m \in \mathbb{N} \) be a positive integer and \( K \subseteq \mathbb{N} \) be a given finite set. There exists a constant \( D = D(m, K) \) such that, for any \( d \in \mathbb{N} \) and \( d > D \) satisfying (2.8), (2.9), and (2.10), an \((m, K, d)\)-pattern exists.

Theorem 2.9 will be proved in §2.8. First, let us observe that if \( (f_i \mid i \in I) \), for some indexing set \( I \), is a family of elements of \( L^*_K(X) \), then

\[
\sum_{i \in I} f_i^{(2)} = \sum_{s=1}^{m} \left( \sum_{i \in I} f_i(x_s)(f_i(x_s) - 1) \right) x_s^2 + \sum_{1 \leq s, t \leq m, i \in I} \sum_{s \neq t} (\sum_{i \in I} f_i(x_s)f_i(x_t)) x_s x_t \tag{2.12}
\]

This can be verified very easily just by expanding the left-hand
side using the definition of $f_i^{(2)}$. With this in mind, we have a very useful lemma.

**Lemma 2.10.** Let $m, d \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. An $(m, K, d)$-pattern on $X = \{x_1, x_2, \ldots, x_m\}$ exists iff there exists a family $(f_i | i \in I)$, for some indexing set $I$, of elements of $L_K(X)$ such that

$$\sum_{i \in I} f_i^{(2)} = d(\sum_{s=1}^{m} x_s)^2.$$ 

The proof of this lemma is straightforward by (2.12) and the definition of an $(m, K, d)$-pattern. This lemma can be rephrased as follows:

**Lemma 2.11.** Let $m, d \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. The existence of an $(m, K, d)$-pattern is equivalent to the existence of a family, $(c_f^d | f \in L_K(X))$, of non-negative integers such that

$$\sum_{f \in L_K(X)} c_f^d f^{(2)} = d(\sum_{s=1}^{m} x_s)^2.$$ 

Sometimes, it is convenient to call such a family an $(m, K, d)$-pattern. However, if we do not restrict ourselves to non-negative integers, then a family, $(c_f^d | f \in L_K(X))$, of integers such that

$$\sum_{f \in L_K(X)} c_f^d f^{(2)} = d(\sum_{s=1}^{m} x_s)^2 \text{ will be called a 'pseudo } (m, K, d)\text{-pattern.' Their existence is provided by}$$
Theorem 2.12. Let $m \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Let $X = \{x_1, x_2, \ldots, x_m\}$ be a set of $m$ symbols. Given any integer $d$, there exists a family, $\{C^d_f \mid f \in L_K(X)\}$, of integers such that

$$\sum_{f \in L_K(X)} C^d_f f(2) = d\left(\sum_{s=1}^{m} x_s\right)^2$$

iff $d$ satisfies (2.8), (2.9), and (2.10).

This theorem will be proved in §2.7.

§2.7 Existence of Pseudo $(m, K, d)$-Pattern. In this section, we will prove Theorem 2.12. In order to prove it, it is necessary to generalize it to

Theorem 2.13. Let $m \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Let $d_{st}$ $(1 \leq s, t \leq m)$ be given integers such that $d_{st} = d_{ts}$ for any $s, t \in I_m$ and $d_{ss}$ is even for any $s \in I_m$. Let

$F = \sum_{1 \leq s, t \leq m} d_{st} x_s x_t$. The necessary and sufficient conditions for the existence of a family, $\{C_f \mid f \in L_K(X)\}$, of integers such that $F = \sum_{f \in L_K(X)} C^d_f f(2)$ are

(i) $\sum_{1 \leq s, t \leq m} d_{st} = 0 \pmod{\beta(K)}$, and

(ii) for each $s \in I_m$, $\sum_{t=1}^{m} d_{st} = 0 \pmod{\alpha(K)}$. (2.13)
Proof of Theorem 2.12: In Theorem 2.13, let \( d_{st} = d \) for all \( s, t \in I_m \). Then \( d \) is even. (2.13) and (2.14) become (2.9) and (2.10), respectively. \( F \) becomes \( F = d \left( \sum_{s=1}^{m} x_s \right)^2 \).

Before we prove Theorem 2.13, let us observe a very elementary but useful fact.

Proposition 2.14. Let \( K \subset \mathbb{N} \) be a given set (finite or infinite). Then there exists a finite set \( K_0 \subset K \) such that \( \alpha(K_0) = \alpha(K) \) and \( \beta(K_0) = \beta(K) \). (Hence \( \gamma(K_0) = \gamma(K) \)).

Proof: By Proposition 1.2, there exist finite subsets \( K_1 \) and \( K_2 \) of \( K \) such that \( \beta(K_1) = \beta(K) \) and \( \alpha(K_2) = \alpha(K) \). Now let \( K_0 = K_1 \cup K_2 \). Then, we have \( \beta(K_0) = \beta(K) \), \( \alpha(K_0) = \alpha(K) \), and hence \( \gamma(K) = \gamma(K_0) \).

In this section, \( K \) will be a subset of \( \mathbb{N} \) such that \( k \geq 3 \) for any \( k \in K \). But it is not necessarily finite. By Proposition 2.14, there exists a finite subset \( K_0 \subset K \) such that \( \alpha(K) = \alpha(K_0) \) and \( \beta(K) = \beta(K_0) \). Assume \( K_0 = \{k_1, k_2, \ldots, k_n\} \). Then there exists \( a_i \in \mathbb{Z} \), \( b_i \in \mathbb{Z} \), \( i \in I_n \) such that \( \beta(K) = \sum_{i=1}^{n} b_i k_i (k_i - 1) \) and \( \alpha(K) = \sum_{i=1}^{n} a_i (k_i - 1) \). We will use these expressions throughout the proof of Theorem 2.13. We will use induction on \( m \) to prove Theorem 2.13.
Proof of Theorem 2.13. For the proof of necessity, let us observe that, if \( f = f(x_1)x_1 + f(x_2)x_2 + \ldots + f(x_m)x_m \) be an element of \( L_K(X) \) where, as usual, \( f(x_s) \) is the coefficient of \( x_s \) in \( f \), then, by setting \( x_s = 1 \) in \( f \) for all \( s \in I_m \), we have

\[
(2) \quad f(1) = \sum_{s=1}^{m} f(x_s)(f(x_s) - 1) + \sum_{1 \leq s, t \leq m \atop s \neq t} f(x_s)f(x_t)
\]

\[
= \left( \sum_{s=1}^{m} f(x_s) \right)^2 - \sum_{s=1}^{m} f(x_s) \tag{2.15}
\]

But \( f \in L_K(X) \) implies that \( \sum_{s=1}^{m} f(x_s) \in K \). Hence, by (2.15), we have \( f(1) \equiv 0 \pmod{\beta(K)} \), by definition of \( \beta(K) \). Now let we set \( x_s = 1, \) for all \( s \in I_m \) in

\[
\sum_{1 \leq s, t \leq m} d_{st}x_s x_t = 0 \pmod{\beta(K)}.
\]

Then \( \sum_{f \in L_K(X)} C_f f(2) \). From \( \sum_{1 \leq s, t \leq m} d_{st}x_s x_t = \sum_{f \in L_K(X)} C_f f(2) \), we have that, if \( s, t \in I_m \) and \( s \neq t \), then \( d_{st} = \sum_{f \in L_K(X)} C_f f(x_s) f(x_t) \) and, if \( s \in I_m \), then \( d_{ss} = \sum_{f \in L_K(X)} C_f f(x_s)(f(x_s) - 1) \). Hence, for any \( s \in I_m \),
\[
\sum_{t=1}^{m} d_{st} = \sum_{f \in L_K(X)} C_f f(x_s)(f(x_s) - 1) + \\
\sum_{t=1}^{m} \sum_{f \in L_K(X)} C_f f(x_s)f(x_t) \\
= \sum_{f \in L_K(X)} C_f f(x_s) \sum_{t=1}^{m} f(x_t) - f(x_s) \\
= \sum_{f \in L_K(X)} C_f f(x_s) \sum_{t=1}^{m} f(x_t) - 1 \\
\tag{2.16}
\]

But \( f \in L_K(X) \) implies \( \sum_{t=1}^{m} f(x_t) \in K \). Hence by (2.16) and the definition of \( \alpha(K) \), \( \sum_{t=1}^{m} d_{st} = 0 \) (mod \( \alpha(K) \)).

To prove sufficiency, use induction on \( m \). For \( m = 1 \), (2.13) and (2.14) become \( d_{11} = 0 \) (mod \( \beta(K) \)), say \( d_{11} = \beta(K) \cdot a \) for some \( a \in \mathbb{Z} \). Let \( h_i = k_i x_1 \) for \( i \in I_n \). Hence, \( h_i \in L_K([x_1]) \) for \( i \in I_n \) and we have \( d_{11}^2 = \sum_{i=1}^{n} a b_i h_i^2 \) by the fact that \( \beta(K) = \sum_{i=1}^{n} b_i k_i (k_i - 1) \).

For \( m = 2 \), (2.13) and (2.14) become

\[
d_{11} + d_{12} + d_{21} + d_{22} = 0 \text{ (mod } \beta(K) \text{)}, \tag{2.17}
\]

\[
d_{11} + d_{12} = 0 \text{ (mod } \alpha(K) \text{)}, \tag{2.18}
\]
\[ d_{21} + d_{22} = 0 \pmod{\alpha(K)}. \]

Thus, \( d_{11} = 2a \) for some \( a \in \mathbb{Z} \) and \( d_{12} = d_{21} \). By (2.18), \( d_{21} = d_{12} = \alpha(K)b - d_{11} \) for some \( b \in \mathbb{Z} \). Recall that

\[ \alpha(K) = \sum_{i=1}^{n} a_{i}(k_{i} - 1) \quad \text{and} \quad k_{i} > 3 \quad \text{for} \quad i \in I_{n}. \]

Define \( f_{i} = 2x_{1} + (k_{i} - 2)x_{2} \) and \( h_{i} = x_{1} + (k_{i} - 1)x_{2} \) for \( i \in I_{n} \).

Thus we have

\[ f_{i}^{(2)} - 2h_{i}^{(2)} = 2x_{1}^{2} - 2(x_{1}x_{2} + x_{2}x_{1}) - (k_{i} - 2)(k_{i} + 1)x_{2}^{2}. \]

Now,

\[ \sum_{i=1}^{n} a_{i}h_{i}^{(2)} = \left( \sum_{i=1}^{n} a_{i}(k_{i} - 1) \right)(x_{1}x_{2} + x_{2}x_{1}) + \left( \sum_{i=1}^{n} a_{i}(k_{i} - 1)(k_{i} - 2) \right)x_{2}^{2}. \]

Thus, since \( \sum_{i=1}^{n} a_{i}(k_{i} - 1) = \alpha(K) \) and

\[ F = d_{11}x_{1}^{2} + d_{12}x_{1}x_{2} + d_{21}x_{2}x_{1} + d_{22}x_{2}^{2}, \]

\[ F - b\left( \sum_{i=1}^{n} a_{i}h_{i}^{(2)} \right) = d_{11}x_{1}^{2} - d_{11}(x_{1}x_{2} + x_{2}x_{1}) + \]

\[ (d_{22} - b\sum_{i=1}^{n} a_{i}(k_{i} - 1)(k_{i} - 2))x_{2}^{2}, \]

by using the fact that \( d_{12} = d_{21} = \alpha(K)b - d_{11} \). But, then, for any fixed \( i_{0} \in I_{n} \), we have
\[ F - b( \sum_{i=1}^{n} a_i h_i(2)) - a(f_1^{(2)} - 2h_1^{(2)}) = \]
\[ = [d_{22} - \sum_{i=1}^{n} a_i (k_i - 1)(k_i - 2)b + (k_i + 1)(k_i - 2)a]x_2^2, \]

by using the fact that \( d_{11} = 2a \). Now,

\[ d_{22} - \sum_{i=1}^{n} a_i (k_i - 1)(k_i - 2)b + (k_i + 1)(k_i - 2)a = \]
\[ = d_{11} + d_{12} + d_{21} + d_{22} - \sum_{i=1}^{n} a_i (k_i - 1)k_i b + k_i (k_i - 1), \]

by using the fact that \( d_{12} = d_{21} = \alpha(K)b - d_{11} \) and

\[ \alpha(K) = \sum_{i=1}^{n} a_i (k_i - 1). \]

Now, by the definition of \( \beta(K) \),

\[ k_i (k_i - 1) \equiv 0 \pmod{\beta(K)} \]

for any \( i \in I_n \). Using (2.17), we have

\[ d_{22} - \sum_{i=1}^{n} a_i (k_i - 1)(k_i - 2)b + (k_i + 1)(k_i - 2)a \equiv 0 \pmod{\beta(K)}. \]

By the case for \( m = 1 \), we have

\[ F - b( \sum_{i=1}^{n} a_i h_i^{(2)}) - a(f_1^{(2)} - 2h_1^{(2)}) = \sum_{j=1}^{v} c_j g_j^{(2)}, \]

where \( c_j \in \mathbb{Z}, g_j \in I_K([x_2]), \) for \( j = 1, 2, \ldots, v \). Therefore,
Let \( m \) be a given positive integer. Assume that the theorem is valid for all \( m' < m \). Consider, as in the case when \( m = 2 \),

\[ f_i = 2x^1 + (k_i - 2)x^m \quad \text{and} \quad h_i = x^1 + (k_i - 1)x^m \quad \text{for} \quad i \in \mathcal{I}_m. \]

Thus, for \( i \in \mathcal{I}_n \),

\[ f_i^{(2)} - 2h_i^{(2)} = 2x^2 - 2(x^1 x^m + x^m x^1) - (k_i - 2)(k_i - 1)x^2. \quad (2.19) \]

Let \( F = \sum_{1 \leq s, t \leq m} d_{st} x^s x^t \in \mathbb{Z}[x^1, x^2, \ldots, x^m] \) be a given element whose coefficients satisfy the hypotheses of Theorem 2.13. Let \( i_0 \in \mathcal{I}_n \) be any fixed element. Define \( g_j = x^1 + x^j + (k_{i_0} - 2)x^m \) for \( j = 2, 3, \ldots, m - 1 \). For notational convenience, let \( g_0 = x^1 + (k_{i_0} - 1)x^m \). Now, define

\[ g = \sum_{j=2}^{m-1} d_{1j} g_j^{(2)} - \left( \sum_{j=2}^{m-1} d_{ij} g_0^{(2)} \right). \]

Consider \( F - g \). The coefficient of \( x^2 \) in \( F - g \) is \( d_{11} \).

The coefficient of \( x^j x^1 + x^1 x^j \) in \( F - g \) is zero for \( j = 2, 3, \ldots, m - 1 \). The coefficient of \( x^1 x^m + x^m x^1 \) in \( F - g \) is

\[ d_{1m} - \left[ \sum_{j=2}^{m-1} d_{1j} (k_{i_0} - 2) - \sum_{j=2}^{m-1} d_{1j} (k_{i_0} - 1) \right] = \sum_{j=2}^{m-1} d_{1j}. \]
Now, using the fact \( \sum_{i=1}^{n} a_i (k_i - 1) = \alpha(k) \),

\[
\sum_{i=1}^{n} a_i h_i^{(2)} = \alpha(k)(x_1 x_{m} + x_{m} x_1) + \sum_{i=1}^{m} a_i (k_i - 1)(k_i - 2)x_m^{2}.
\]

By (2.14), we have

\[
d_{12} + d_{13} + \ldots + d_{lm} = \alpha(k)b - d_{11},
\]

for some \( b \in \mathbb{Z} \). Consider \( F - g - b \sum_{i=1}^{n} a_i h_i^{(2)} \). The coefficient of \( x_1^2 \) is still \( d_{11} \). However, the coefficient of \( x_1 x_m + x_m x_1 \) is \(-d_{11}\) by (2.2). Now let \( d_{11} = 2a \) for some \( a \in \mathbb{Z} \).

Consider \( G = F - g - b \sum_{i=1}^{n} a_i h_i^{(2)} - a_i h_i^{(2)} - 2h_i^{(2)} \). Then, by (2.19), the coefficients of \( x_1^2 \) and \( x_1 x_m + x_m x_1 \) are zero, i.e. there is no terms involving \( x_1 \) in \( G \). Hence \( G \in \mathbb{Z}[x_2, x_3, \ldots, x_m] \). Write \( G = \sum d_{st} x_s x_t \) where \( 1 \leq s, t \leq m \).

\( d_{st} = 0 \) if one of \( s \) and \( t \) is 1.

Let us observe now that, given \( f, g \in \mathbb{Z}[x_1, x_2, \ldots, x_m] \), if the coefficients of both \( f \) and \( g \) satisfy the hypotheses of Theorem 2.13, then so do the coefficients of \( f + g \) and \( cf \) for any \( c \in \mathbb{Z} \). Now, \( g_j^{(2)} \in \mathbb{Z}[x_1, x_2, \ldots, x_m] \) for \( j = 2, 3, \ldots, m - 1 \), \( h_i^{(2)} \in \mathbb{Z}[x_1, x_2, \ldots, x_m] \) for \( i \in I_n \), and \( f_i^{(2)}, g_i^{(2)} \in \mathbb{Z}[x_1, x_2, \ldots, x_m] \). And, they all satisfy the hypotheses of Theorem 2.13. Hence \( G \)
satisfy the hypotheses of Theorem 2.13. Thus,
\[ \sum_{1 \leq s, t \leq m} d'_{st} \equiv 0 \pmod{\beta(K)} \] and, for any \( s \in I_m \),
\[ \sum_{t=1}^{m} d'_{st} \equiv 0 \pmod{\alpha(K)}. \] But \( d' = 0 \) if either \( s \) or \( t \) is
\[ s \in \{2, 3, \ldots, m\}, \sum_{t=2}^{m} d'_{st} \equiv 0 \pmod{\alpha(K)}. \] By induction hypotheses,
\[ G = \sum_{f \in L_K(X')} c_f^{(2)} \] for some family, \((c_f | f \in L_K(X'))\), of
integers where \( X' = \{x_2, x_3, \ldots, x_m\}. \) But, then,
\[ F = \sum_{f \in L_K(X)} c_f^{(2)} \] for some family, \((c_f | f \in L_K(X))\), of integers.
By induction, we have the result, i.e. a 'pseudo \((m, K, d)\)-pattern' exists.

§2.8 Proof of the Existence Theorem for \((m, K, d)\)-Pattern.
In this section, we will devote ourselves to proving Theorem 2.9.
\( K \subseteq \mathbb{N} \) will be assumed to be a finite set.

Let \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. An integer \( d \) is said to
be admissible \underline{iff} \( d \) satisfied (2.8), (2.9), and (2.10). By
Theorem 2.12, for every admissible \( d \), there exists a family
\((c_f^d | f \in L_K(X))\), of integers such that
\[ d \left( \sum_{s=1}^{m} x_s \right)^2. \] To prove Theorem 2.9, let us first assume that there
exists, for some \( d_0 > 0 \), an \((m,K,d_0)\)-pattern \((C^d_f | f \in L_K(X))\) such that \( C^d_f > 0 \) for every \( f \in L_K(X) \).

Consider the set of all admissible integers \( d \) such that \(-d_0 < d \leq 0\). Let us denote it by \( S \). Clearly \( S \neq \emptyset \) since \( 0 \in S \). For any \( d \in S \), not all of \( C^d_f \)'s are strictly positive.

Put \( D'_o = \min\{C^d_f | d \in S, f \in L_K(X)\} \). Then \( D'_o \leq 0 \). Let \( D_o = -d_0 D'_o \). Then \( D_o \geq 0 \).

We now claim that an \((m,K,d)\)-pattern exists for all admissible \( d \geq D_o \). Observe first that if \( d_1 \) and \( d_2 \) are admissible integers, then \( d_1 + d_2 \) and \( a d_1 \) are admissible too, for any \( a \in \mathbb{Z} \).

Let \( d \geq D_o \) be a given admissible integer. Thus, \( d \geq 0 \). Write \( d = D_o + d' \) for some \( d' \in \mathbb{N}_0 \). Hence we have \(-d' = d_o s + t\) where \( s \) is a nonpositive integer and \( 0 \leq t < d_o \). Thus, \( d' = d_o (-s) + (-t) \) where \(-d_o < -t \leq 0\). Therefore, \( d = a d_o + b \) where \( a \in \mathbb{N}_0 \) and \(-d_o < b \leq 0\). Since both \( d \) and \( d_o \) are admissible, so is \( b \). Thus, \( b \in S \). Therefore, we have

\[
\sum_{f \in L_K(X)} C^d_f f(2) = d_o \left( \sum_{s=1}^{m} x_s \right)^2 ,
\]

\[
\sum_{f \in L_K(X)} C^b_f f(2) = b \left( \sum_{s=1}^{m} x_s \right)^2 , \text{ and}
\]

\[
\sum_{f \in L_K(X)} C^d_f f(2) = d \left( \sum_{s=1}^{m} x_s \right)^2 .
\]
where \( C_f^d = aC_f^0 + C_f^b \) for each \( f \in L_K(X) \).

Now, \( ad_o \geq d > D_o = -d_0D'_o \). Since \( d_0 > 0 \), \( a \geq -D'_o \geq -C_f^b \) for every \( f \in L_K(X) \), by definition of \( D'_o \). Now, since \( a > 0 \) and \( C_f^0 > 0 \) for every \( f \in L_K(X) \), \( aC_f^0 + C_f^b > 0 \), i.e. \( C_f^d > 0 \) for every \( f \in L_K(X) \). By Lemma 2.11, an \((m,K,d)\)-pattern exists.

To complete the proof of Theorem 2.9, it remains to exhibit, for some \( d > 0 \), an \((m,K,d)\)-pattern \((C_f^d | f \in L_K(X))\) such that \( C_f^d > 0 \) for every \( f \in L_K(X) \), and \( \sum_{f \in L_K(X)} C_f^d(f^{(2)}) = d(\sum_{s=1}^{m} x_s)^2 \).

To do so, let us consider

\[
F = \sum_{f \in L_K(X)} f^{(2)}.
\]

By symmetry, we have, since \( K \) is finite,

\[
F = a(\sum_{s=1}^{m} x_s)^2 + b(\sum_{s=1}^{m} x_s^2), \tag{2.21}
\]

for some \( a, b \in \mathbb{Z} \).

Since all the coefficients of \( f \) are nonnegative for every \( f \in L_K(X) \), we have \( a \geq 0 \). If \( k \in K \), then \( x_1 + x_2 + (k-2)x_3 \in L_K(X) \) and hence \( a > 0 \). If \( b = 0 \) in (2.21), then, by Lemma 2.11, an \((m,K,a)\)-pattern exists with \( C_f^a = 1 \) for every \( f \in L_K(X) \).

Suppose that \( b < 0 \). Let \( k \in K \) be any fixed element. Define
\[ G = \sum_{s=1}^{m} (k x_s)^{(2)}. \]

Then \( G = k(k - 1) \sum_{s=1}^{m} x_s^2 \) and \( k x_s \in L_k(X) \) for \( s = 1, 2, \ldots, m \).

Hence, we have \( k(k - 1)F - bG = ak(k - 1)(\sum_{s=1}^{m} x_s^2) \). Thus, we have a family, \( (C_f \mid f \in L_k(X)) \), of positive integers such that

\[ \sum_{f \in L_k(X)} C_f f^{(2)} = ak(k - 1)(\sum_{s=1}^{m} x_s^2) \]

where \( C_f = k(k - 1) \) if \( f \notin \{k x_1, k x_2, \ldots, k x_m\} \) and \( C_f = k(k - 1) - b \) if \( f \in \{k x_1, k x_2, \ldots, k x_m\} \). Note that, since \( b < 0 \), \( k(k - 1) - b > 0 \).

Therefore, an \((m, K, ak(k - 1))\)-pattern exists.

Now, the only case left to be shown is the case when \( b > 0 \).

Let \( k \in K \) be any fixed element. Recall that \( k \geq 3 \) and \( m \geq 2 \).

Let us write \( k = mu + c \) where \( u \geq 0 \) and \( 0 \leq c < m \).

**Case 1.** \( c = 0 \). Consider \( ux_1 + ux_2 + \ldots + ux_m \). Then it is in \( L_k(X) \). Define

\[ G = (ux_1 + ux_2 + \ldots + ux_m)^{(2)}. \]

Then \( G = u^2(\sum_{s=1}^{m} x_s^2) - u(\sum_{s=1}^{m} x_s^2) \). Hence we have

\[ uF + bG = (au + bu^2)(\sum_{s=1}^{m} x_s^2). \]

Thus, we have a family, \( (C_f \mid f \in L_k(X)) \), of positive integers such that
\[ \sum_{f \in L_K(X)} C_f f(2) = (au + bu^2)(\sum_{s=1}^{m} x_s)^2 \]

where \( C_f = u \) if \( f \neq u_1 + u_2 + \ldots + u_m \) and \( C_f = u + b \) if \( f = u_1 + u_2 + \ldots + u_m \).

Therefore an \((m, K, au + bu^2)\)-pattern exists.

**Case 2.** \( c = 1 \). Consider \( g_i = \sum_{s=1}^{m} r_s^i x_s \) where \( r_s^i = u \)

if \( s \neq i \) and \( r_s^i = u + 1 \), for \( i = 1, 2, 3, \ldots, m \). Then

\( g_i \in L_K(X) \subseteq L_K(X) \) for \( i \in I_m \). Define

\[ G = \sum_{i=1}^{m} g_i^{(2)}. \]

Then we have \( G = (2u(u + 1) + (m - 2)u^2)(\sum_{s=1}^{m} x_s)^2 - mu \sum_{s=1}^{m} x_s^2 \).

Hence we have \( muF + bG = (mua + 2u(u + 1)b + (m - 2)u^2b)(\sum_{s=1}^{m} x_s)^2 \).

Let \( d = mua + 2u(u + 1)b + (m - 2)u^2b \). Then, we have a family,

\( (C_f | f \in L_K(X)) \), of positive integers such that

\[ \sum_{f \in L_K(X)} C_f f(2) = d(\sum_{s=1}^{m} x_s)^2 \]

where \( C_f = mu \) if \( f \notin \{g_1, g_2, \ldots, g_m\} \) and \( C_f = mu + b \) if \( f \in \{g_1, g_2, \ldots, g_m\} \).

Therefore, an \((m, K, d)\)-pattern exists.

**Case 3.** \( c \geq 2 \). In this case, \( m \) must be at least 3. Let \( P_c(X) \) be the class of all \( c \)-subsets of \( X \). For any \( A \in P_c(X) \), define \( g_A \) in such a way that \( g_A = \sum_{s=1}^{m} a_s^A x_s \) where \( a_s^A = u + 1 \)

if \( x_s \in A \) and \( a_s^A = u \) if \( x_s \notin A \). Clearly, \( g_A \in L_K(X) \subseteq L_K(X) \)
for every $A \in P_c(X)$. Define

$$G = \sum_{A \in P_c(X)} g_A^{(2)}.$$  

Then, by easy computation, we have

$$G = A(\sum_{s=1}^{m} x_s^2) - B(\sum_{s=1}^{m} x_s^2)$$

where

$$A = (m - 2)u^2 + 2(m - 2)u(u + 1) + (m - 2)(u + 1)^2,$$

and

$$B = \binom{m}{c}u + \binom{m - 2}{c - 2}.$$  

Hence we have $BF + bG = (aB + bA)(\sum_{s=1}^{m} x_s^2)$. Let $d = aB + bA$

and $E = \{ g_A \mid A \in P_c(X) \}$. Hence we have a family, $(C_f \mid f \in L_K(X))$

of positive integers such that $\sum_{f \in L_K(X)} C_f^{(2)} = d(\sum_{s=1}^{m} x_s^2)$ where

$C_f = B$ if $f \notin E$ and $C_f = B + b$ if $f \in E$. Therefore,

an $(m,K,d)$-pattern exists.

This completes the proof of Theorem 2.9.

\textbf{2.9 $\beta(NG[m,K])$.} In this section, we shall prove one of our main results, namely

**Theorem 2.15.** Let $m \in \mathbb{N}$ be a given integer. Let $K \subseteq \mathbb{N}$ be a finite set such that $k \geq 3$ for any $k \in K$. Then
\[
\beta(NG[m,K]) = \beta(m,K),
\]

where \( \beta(m,K) = \varepsilon \left( \frac{\beta(K)}{(m^2,\gamma(K))(m,\alpha(K))} \right) \).

Theorem 2.15 will be proved latter. We shall make several references to a most remarkable theorem on prime numbers proved by G. L. Dirichlet in 1837. So, we state it now.

\textbf{Theorem 2.16 (Dirichlet).} If \( x,y \in \mathbb{Z} \) and \( (x,y) = 1 \), then the set \( D = \{x + ky \mid k \in \mathbb{N} \} \) contains infinitely many prime numbers.

In view of Proposition 2.8, we may restate Theorem 2.9 as

\textbf{Theorem 2.9'.} Let \( m \in \mathbb{N} \) be a given integer and \( K \subseteq \mathbb{N} \) be a given finite set. Then there exists a constant \( T = T(m,K) \) such that, for any \( t \in \mathbb{N} \) with \( t > T \), an \( (m,K,t\beta(m,K)) \)-pattern exists.

Let \( T(m,K) \) be the smallest integer for which Theorem 2.9' holds.

In order to establish Theorem 2.15, let us observe a very useful lemma.

\textbf{Lemma 2.17.} Let \( d,c \in \mathbb{N} \). Assume that \( d \) is even. Define the set \( Q = \{q \in \mathbb{N} \mid q, \text{ a prime power, } q > c, q \equiv d + 1 \pmod{2d} \} \).

Then \( \beta(Q) = d \).

\textbf{Proof:} For any \( q \in Q \), \( d \mid q(q - 1) \). Thus, \( d \mid \beta(q) \), say \( \beta(Q) = ds \) for some \( s \in \mathbb{N} \). We claim that \( s = 1 \). Assume not.

Let \( p \) be a prime divisor of \( s \).
Now, observe first that either \((2dp, d(2p + 1) + 1) = 1\) or \((2dp, d(2p - 1) + 1) = 1\). Indeed, suppose \((2dp, d(2p + 1) + 1) = u \neq 1\) and \((2dp, d(2p - 1) + 1) = v \neq 1\) for some \(u, v \in \mathbb{N}\). Let \(p'\) be a prime divisor of \(u\). Then \(p' | 2dp\) and \(p' | d(2p + 1) + 1\).

Since \(p' | d(2p + 1) + 1\) and \(d\) is even, \(p'\) is not even. Thus \(p' | dp\). Suppose that \(p' | d\). Then, since \(p' | d(2p + 1) + 1\), we have that \(p' | l\), a contradiction. Thus \(p' = p\), i.e., \(p | d(2p + 1) + 1\).

Similarly, \(p | d(2p - 1) + 1\).

Now, \(p | d(2p + 1) + 1 = 2dp + d + 1\) implies that \(p | d + 1\).

Similarly, \(p | d - 1\). That is, \(p | (d + 1) - (d - 1) = 2\) and we have that \(p = 2\). Thus \(p = 2 | d + 1\), a contradiction since \(d\) is even.

Thus either \((2dp, d(2p + 1) + 1) = 1\) or \((2dp, d(2p - 1) + 1) = 1\).

Without loss of generality, let us assume \((2dp, d(2p + 1) + 1) = 1\).

By Dirichlet's Theorem (2.16), there exists a prime number \(q = 2dpt + d(2p + 1) + 1 > \max(c, \beta(q))\) for some \(t \in \mathbb{N}\). Thus we have \(q \equiv d + 1 \mod 2d\) and \(q \in Q\), i.e., \(\beta(q) | q(q - 1)\).

Since \(q\) is prime and \(\beta(q) < q\), \(\beta(q) | q - 1\). Thus \(ds | 2dpt + 2pd + d\), i.e., \(s | 2pt + 2p + 1\). Since \(p | s\), we have \(p | 2p(t + 1) + 1\), a contradiction. Therefore \(s = 1\), i.e., \(\beta(q) = d\).

Proof of Theorem 2.15. In view of Theorem 2.9', let \(p_1, p_2 \in \mathbb{N}\) be two distinct prime numbers such that \(\min(p_1, p_2) > T(m, K)\) obtained in Theorem 2.9'. Then \((m, K, p_1\bar{\beta}(m, K))\)-pattern exists and \((m, K, p_2\bar{\beta}(m, K))\)-pattern exists. Define the set...
\[ Q_1 = \{ q \in \mathbb{N} \mid q, \text{a prime power}, q > \frac{k_0(k_0-1)}{d_1}, q \equiv d_1 + 1 \text{ (mod } 2d_1) \}, \]

\[ Q_2 = \{ q \in \mathbb{N} \mid q, \text{a prime power}, q > \frac{k_0(k_0-1)}{d_2}, q \equiv d_2 + 1 \text{ (mod } 2d_2) \}, \]

where \( k_0 = \max(K) \), \( d_1 = p_1\bar{\beta}(m,K) \), and \( d_2 = p_2\bar{\beta}(m,K) \). By Theorem 2.6, \( Q_1 \subseteq \text{NG}[m,K] \) and \( Q_2 \subseteq \text{NG}[m,K] \). Hence \( \beta(\text{NG}[m,K]) \mid \beta(Q_1) = d_1 \) and \( \beta(\text{NG}[m,K]) \mid \beta(Q_2) = d_2 \). Now we have \( \beta(\text{NG}[m,K]) \mid (d_1, d_2) = \bar{\beta}(m,K) \).

For any \( n \in \text{NG}[m,K] \), we have, by Proposition 2.2, \( n(n - 1) \equiv 0 \text{ (mod } \bar{\beta}(m,K)) \). Thus, \( \bar{\beta}(m,K) \mid \beta(\text{NG}[m,K]) \). Therefore, \( \beta(\text{NG}[m,K]) = \bar{\beta}(m,K) \), as desired.

We may remove the restriction 'K is finite' in Theorem 2.15. In fact, we have

**Theorem 2.18.** Let \( m \in \mathbb{N} \) be given and \( K \subseteq \mathbb{N} \) be a set of positive integers greater than or equal to 3. Then

\[ \beta(\text{NG}[m,K]) = \bar{\beta}(m,K). \]

**Proof:** By Proposition 2.14, let \( K_0 \subseteq K \) be a finite set such that \( \beta(K_0) = \beta(K), \alpha(K_0) = \alpha(K), \) and \( \gamma(K_0) = \gamma(K) \). Thus \( \bar{\beta}(m,K_0) = \bar{\beta}(m,K) \). Now, \( \text{NG}[m,K_0] \subseteq \text{NG}[m,K] \). Hence
\[ \beta(NG[m,K]) \mid \beta(NG[m,K_0]) = \beta(m,K_0) = \beta(m,K) , \text{ by Theorem 2.15} . \]

By Proposition 2.2, we have that \( \beta(m,K) \mid \beta(NG[m,K]) \). Thus we have that \( \beta(NG[m,K]) = \beta(m,K) \).

One of the main results in [26, 27] is

**Theorem 2.19.** Let \( K \) be a closed set. Then there exists a constant \( c \) such that for any \( k \in K \),
\[
\{ v \mid v \geq c, \ v \equiv k \pmod{\beta(K)} \} \subseteq K .
\]

Since \( NG[m,K] \) is closed set, we have, by Theorem 2.18, a consequence of Theorem 2.19

**Theorem 2.20.** Let \( K \subseteq N \) and \( m \in N \) be given. Then there exists a constant \( c \) such that for any \( k \in NG[m,K] \),
\[
\{ n \mid n \geq c, \ n \equiv k \pmod{\beta(m,K)} \} \subseteq NG[m,K] .
\]

In particular, since \( 1 \in NG[m,K] \), \( NG[m,K] \) contains all sufficiently large integers \( n \equiv 1 \pmod{\beta(m,K)} \). Clearly, \( \beta(m,K) \mid k(k - 1) \), for all \( k \in K \). Thus, we also have that \( NG[m,K] \) contains all sufficiently large integers \( n \equiv 1 \pmod{k(k - 1)} \).
CHAPTER III

EXISTENCE OF GD(n,m,K,λ)

§3.1 A Construction. In this chapter, we will devote ourselves to computing \( \alpha(NG[m,K]) \), i.e., to proving that 
\( \alpha(NG[m,K]) = \overline{\alpha}(m,K) \). We shall write \( \overline{\alpha}(m,k) \) instead of 
\( \overline{\alpha}(m,k,J) \). Recall that 
\( \overline{\alpha}(m,K) = \frac{\alpha(K)}{(m,\alpha(K))} \). Thus,
\[ \overline{\alpha}(m,k) = \frac{k - 1}{(m,k - 1)} \]. First of all, we would like to show that 
\( \alpha(NG[m,k]) = \overline{\alpha}(m,k) \). Then we will use the result to prove that 
\( \alpha(NG[m,K]) = \overline{\alpha}(m,K) \).

In order to prove that \( \alpha(NG[m,k]) = \overline{\alpha}(m,k) \), we need a construction of a GDD from a given GDD with the aid of a finite dimensional vector space over a finite field. The technique employed in [27] for PBD can be generalized to GDD in the following way.

Let \( d, q, \) and \( n \) be given positive integers such that \( q \) is a prime power and \( d \geq n^2 \). Let \( F = GF(q) \) be the finite field of \( q \) elements. Let \( V \) be a \( d \)-dimensional vector space over \( F \). Let \( m,k \in \mathbb{N} \) be given. Consider \( X = I_m \times I_n \). Let \( G_i = I_m \times \{i\} \) for each \( i \in I_n \). Consider \( \mathcal{B} = \{ G_i \mid i \in I_n \} \). Let \( (X,\mathcal{B},\mathcal{A}) \) be a GD(n,m,k,q), say \( \mathcal{A} = \{ B_i \mid i \in I \} \) for some indexing set \( I \).
As we observed in Chapter I, \( l \in \mathbb{N}[m,k] \) for any \( m \in \mathbb{N} \). We may assume that \( n > 1 \). Before we exhibit the construction, let us first observe

**Proposition 3.1.** There exist linear transformations \( f_1, f_2, \ldots, f_n \) of \( V \) over \( F \) such that \( f_s - f_r \) is nonsingular for any \( r, s \in I_n \) with \( r < s \), and any non-zero linear combination of

\[
(f_t - f_1)^{-1}, (f_t - f_2)^{-1}, \ldots, (f_t - f_{t-1})^{-1}
\]

is also nonsingular for \( t = 2, 3, \ldots, n \).

**Proof:** Let \( E \supseteq F \) be an extension with \( [E:F] = d \). Let \( \theta \) be the generator of the cyclic group \( F^* = F - \{0\} \). Then \( E = F(\theta) \).

Since \( [E:F] = d \), \( \theta \) is algebraic over \( F \). Then there is a unique monic irreducible polynomial \( p(x) \in F[x] \) such that \( \deg p(x) = d \) and \( p(\theta) = 0 \). Consider the companion matrix \( c(p) \) of \( p(x) \). We may view \( c(p) \) as a linear transformation \( T: V \rightarrow V \) over \( F \).

Then \( T \) has \( p(x) \) as its minimal polynomial which is irreducible (i.e. \( p(T) = 0 \), zero linear transformation which maps \( V \) onto \( \{0\} \), and it is of least degree).

Let \( g(x) \in F[x] \) be any nonzero polynomial with \( \deg g(x) < d \).

Since \( p(x) \) is irreducible, \( (g(x), p(x)) = 1 \) and, hence,

\[
f(x)g(x) + h(x)p(x) = 1 \quad \text{for some} \quad f(x), h(x) \in F[x].
\]

Hence \( f(T)g(T) = I \) where \( I: V \rightarrow V \) is the identity transformation. Thus, \( g(T) \) is nonsingular if \( g(T) \) is a polynomial in \( T \) of
degree < d.

Define \( f_r = T^r \) for \( r = 1, 2, \ldots, n \). Then \( f_s - f_r \), for \( 1 \leq r < s \leq n \), is a polynomial in \( T \) with degree < d. Hence it is nonsingular.

Now suppose that, for some \( t, 2 \leq t \leq n \), and some \( a_r \in F \), \( r = 1, 2, \ldots, t-1 \), the linear transformation \( L = \sum_{r=1}^{t-1} a_r (f_t - f_r)^{-1} \) is singular. Consider the linear transformation

\[
g(T) = L(f_t - f_1)(f_t - f_2) \ldots (f_t - f_{t-1}) \cdot
\]

Then \( g(T) \) is also singular. Now observe that, since \( f_r = T^r \) for \( r = 1, 2, \ldots, n \), \((f_s - f_r)'s\) commute with each other. Hence

\[
g(T) = \sum_{r=1}^{t-1} a_r \prod_{1 \leq s \leq t-1 \atop r \neq s} (T - T^s).
\]

It is a polynomial in \( T \) of degree \( t(t-2) < n^2 \leq d \). Thus, \( g(T) = 0 \), the zero transformation. Now observe that the coefficient of

\[
\prod_{1 \leq s \leq t-1 \atop r \neq s} T^s = \frac{1}{T^r} T^{t(t-1)-r}
\]

in \( g(T) \) is \((-1)^{t-2} a_r \). Therefore, \( a_r = 0 \) for \( r = 1, 2, \ldots, t-1 \). Hence, any nonzero linear combination \( L \)
is nonsingular for $t = 2, 3, ..., n$.

We will use these $f_r$'s found in the previous proposition throughout this section. Let $W \subseteq V$ be a hyperplane (i.e. a $(d-1)$-dimensional subspace). Define $W_{rs} = (f_s - f_r)(W)$ for $1 \leq r < s \leq n$. Hence $\dim W_{rs} = d - 1$. Let $C_{rs} = V/W_{rs}$, the quotient space (i.e. the class of cosets of $W_{rs}$). Then $|C_{rs}| = q$. Recall the GD$(n,m,k,q)$ $(X,\mathcal{A})$ where $X = I_m \times I_n$, $\mathcal{A} = \{I_m \times \{i\} | i \in I_n\}$, and $\mathcal{A} = (B_i | i \in I)$ for some indexing set $I$. With this terminology in mind, we have

**Proposition 3.2.** There exists a system of mappings $\mu_i : B_i \to V$, $i \in I$ such that, for any $(a,r), (b,s) \in X$ with $r < s$, the elements $\mu_i(b,s) - \mu_i(a,r)$, $i \in I$ form a system of representatives for $C_{rs}$.

**Proof:** Let $g : V \to F$ be a linear functional with kernel $W$. Thus, $g$ is not the zero functional. For any $r, s \in I_n$ with $r < s$, let $g_{rs} = g_{o}(f_s - f_r)^{-1}$. By definition of $W_{rs}$, the kernel of $g_{rs}$ is $W_{rs}$. Now, we claim that for each $t$, $2 \leq t \leq n$, the functionals $g_{rt}$, $r = 1, 2, ..., t-1$, are linearly independent.

Suppose that, for some $t$, $2 \leq t \leq n$, and some $a_r \in F$, $r = 1, 2, ..., t-1$, we have $\sum_{r=1}^{t-1} a_r g_{rt} = 0$, the zero functional.

Then $g_{o}(\sum_{r=1}^{t-1} a_r (f_t - f_r)^{-1}) = 0$. Hence, $\sum_{r=1}^{t-1} a_r (f_t - f_r)^{-1}$ maps $V$ onto $W$, i.e. $\sum_{r=1}^{t-1} a_r (f_t - f_r)^{-1}$ is singular. By
Proposition 3.1, \( a_r = 0 \) for \( r = 1, 2, \ldots, t - 1 \), as claimed.

Now \( g_{rs} : V \rightarrow F \) is a linear functional with kernel \( W_{rs} \).

By a fundamental theorem in linear algebra, \( V/W_{rs} = C_{rs} \) is in one-to-one correspondence with \( F \). In fact, \( v_1 \) and \( v_2 \) are in the same coset of \( W_{rs} \) iff \( g_{rs}(v_1) = g_{rs}(v_2) \). (More algebraically, \( C_{rs} \) is isomorphic to \( F \) as a vector space.)

For each pair \((a,r)\) and \((b,s)\) of \( X \) not in the same group of \( \mathcal{G} \), say \( r < s \), the number of indices \( i \in I \) such that \((a,r),(b,s) \in B_i \) is precisely \( q \), since \((X,\mathcal{G},\mathcal{C})\) is a \( GD(n,m,k,q) \). We can define an one-to-one correspondence between \( F \) and the set of indices \( i \in I \) such that \((a,r),(b,s) \in B_i \).

For notational convenience, let \( e_{(a,r),(b,s)}(i) \) denote the image of \( i \) in \( F \) under the one-to-one correspondence, for each fixed pair \((a,r),(b,s)\) of \( X \) with \( r < s \). Hence,

\[
F = \{e_{(a,r),(b,s)}(i) \mid i \in I, (a,r),(b,s) \in B_i\}, \quad (3.1)
\]

for any pair \((a,r),(b,s)\) of \( X \) with \( r < s \).

For each \( i \in I \), define \( \mu_i : B_i \rightarrow V \) inductively. Define an ordering on \( B_i \) by

\[(a,r) < (b,s) \text{ if } r < s,\]

for any \((a,r),(b,s) \in B_i \). Since \( |B_i| = k \), we can find a least element of \( B_i \). Define the image of it under \( \mu_i \) arbitrarily.
Now let \((b, s) \in B_i\). Suppose \(\mu_1\) has been defined for all smaller elements of \(B_i\) than \((b, s)\). Consider the nonhomogeneous system of linear equations in the unknown vector \(\mu_1(b, s)\)

\[
g_{rs}(\mu_1(b, s)) = e_{(a, r)(b, s)}(i) + g_{rs}(\mu_1(a, r)),
\]

for all \((a, r) \in B_i\) such that \((a, r) < (b, s)\).

The system (3.2) of linear equations has a solution since the right-hand side is already defined and \(g_{rs}, r = 1, 2, \ldots, s - 1\), are linearly independent by what we observed previously. Hence we can define, for each \(i \in I\), \(\mu_1: V \to F\) such that (3.2) is valid for all pairs \((a, r), (b, s) \in B_i, r < s\).

From (3.2), we have, for each \(i \in I\), that

\[
g_{rs}(\mu_1(b, s) - \mu_1(a, r)) = e_{(a, r)(b, s)}(i),
\]

for all \((a, r), (b, s) \in B_i, r < s\). But (3.1) tells us that, since the kernel of \(g_{rs}\) is \(W_{rs}\), we have that, for any \((a, r), (b, s) \in X\) with \(r < s\), the elements \(\mu_1(b, s) - \mu_1(a, r)\) for \(i \in I\), form a system of representative for \(C_{rs}\) by (3.3).

We will use these \(\mu_1\)'s, \(i \in I\) throughout this section.

Consider the following sets:

\[
V(a, r) = \{(a, r)\} \times V, \text{ for all } (a, r) \in X,
\]

\[
X^* = \bigcup_{(a, r) \in X} V(a, r),
\]
\[ G_r^* = \bigcup_{a=1}^{m} V(a,r) \quad \text{for} \quad r \in I_n, \]

\[ \mathcal{S}^* = \{ G_r^* | r \in I_n \}. \]

For notational convenience, we shall write any element of \( X^* \) as \((a,r,v)\) instead of \(((a,r),v)\). For each triple \((i,w,v) \in I \times W \times V\), define a \(k\)-subset of \( X^* \) by

\[ A_{i,w,v} = \{(a,r,\mu_1(a,r) + f_r(w) + v) \in X^* | (a,r) \in B_i\}. \]

Let \( \mathcal{A}^* = \{ A_{i,w,v} | (i,w,v) \in I \times W \times V \} \). We claim that \((X^*, \mathcal{S}^*, \mathcal{A}^*)\) is a GD\(n,mq^d,k)\).

Since \( V \) is a \(d\)-dimensional vector space over \( F = GF(q) \), we see that \(|G_r^*| = mq^d\) for \( r \in I_n \). Let \((a,r,x),(b,s,y) \in X^* \) be given. They are contained in the same group of \( \mathcal{S}^* \) iff \( r = s \).

Now assume that \( r < s \). We claim that they are contained in a unique block of \( \mathcal{A}^* \).

Observe that they are contained in \( A_{i,w,z} \) iff \((a,r),(b,s) \in B_i \) and

\[ \mu_1(a,r) + f_r(w) + z = x, \quad (3.4) \]
\[ \mu_1(b,s) + f_s(w) + z = y. \quad (3.5) \]

However, \((3.4)\) and \((3.5)\) are equivalent to \((3.4)\) and

\[ (\mu_1(b,s) - \mu_1(a,r)) + (f_s - f_r)(w) = y - x. \quad (3.6) \]
Now, $y - x$ is in some coset of $W_{rs}$, say $W_{rs} + t$ for some $t \in V$. By Proposition 3.2, there is a unique $i \in I$ such that $(a, r), (b, s) \in B_i$, and $\mu_i(b, s) - \mu_i(a, r)$ is in the coset $W_{rs} + t$. But then $(y - x) - (\mu_i(b, s) - \mu_i(a, r)) \in W_{rs} = (f_s - f_r)(w)$. Since $f_s - f_r$ is nonsingular, there is a unique $w \in W$ such that (3.6) is valid. Then, there is a unique $z \in V$ such that (3.4) is valid. This completes the proof of the following useful

**Theorem 3.3.** Let $m, n, k,$ and $q$ be given positive integers such that $q$ is a prime power. Let $d \in \mathbb{N}$ with $d \geq n^2$.

Suppose a $GD(n, m, k, q)$ exists. Then a $GD(n, mq^d, k)$ exists.

§3.2 $\alpha(NG[m, k])$. In this section, we will prove that $\alpha(NG[m, k]) = \overline{\alpha}(m, k)$, i.e. $\alpha(NG[m, k]) = \frac{k - 1}{(m, k - 1)}$. For notational convenience, we shall write, in this section, $\beta$ and $\alpha$ instead of $\beta(NG[m, k])$ and $\alpha(NG[m, k])$, respectively. As we remarked in §1.3, $oa(k)$ is the smallest integer such that if $s > ao(k)$ is a given positive integer, then $GD(k, s, k)$ exists. First of all, let us observe several lemmas which will be used to prove

$$\alpha = \frac{k - 1}{(m, k - 1)}.$$

**Lemma 3.4.** $\alpha | (\beta, k - 1)$

**Proof:** By the definitions of $\alpha$ and $\beta$, $\alpha | \beta$. By the remark after Theorem 2.20, there exists a constant $C = C(m, k)$ such that
for every $t > C$, a $GD(\beta t + 1, m, k)$ exists. Now choose

$t \in \mathbb{N}$ in such a way that $t > C$ and $(\beta t + 1)m > o\alpha(k)$. Applying

Lemma 1.17 (breaking up groups) with $v = (\beta t + 1)mk$, $K = \{k\}$,

$M' = \{(\beta t + 1)m\}$, $M = \{m\}$, and $\lambda = \lambda' = 1$, we have

$(\beta t + 1)mk \in G_{\{k\}}[[m]]$, i.e. $(\beta t + 1)k \in NG[m,k]$. Hence

$\alpha | \beta kt + k - 1$, i.e. $\alpha | k - 1$, since $\alpha | \beta$. Therefore,

$\alpha | (\beta, k - 1)$, as desired.

Recall that, in Chapter II, we have shown that

$\beta(NG[m,k]) = \overline{\beta}(m,k)$. In particular $\beta = \overline{\beta}(m,k) = e\left(\frac{k(k - 1)}{\binom{m, k}{2} (m, k - 1)}\right)$

where $e(x) = 2x$ if $x$ is odd and $= x$ if $x$ is even. We have, as a consequence of Lemma 3.4, the following

Lemma 3.5. If $\beta = \frac{k(k - 1)}{\binom{m, k}{2} (m, k - 1)}$, then $\alpha = \frac{k - 1}{(m, k - 1)}$.

Proof: Consider

$(\beta, k - 1) = \left(\frac{k(k - 1)}{\binom{m, k}{2} (m, k - 1)}, k - 1\right)$.

Since $(k, k - 1) = 1$, $(\beta, k - 1) = \frac{k - 1}{(m, k - 1)}$. Equation (2.4), for

$K = \{k\}$, implies that $\frac{k - 1}{(m, k - 1)} | \alpha$. By Lemma 3.4, $\alpha = \frac{k - 1}{(m, k - 1)}$.

Proposition 3.6. If $m = k - 1$, then $\alpha = 1$,

(i.e. $\alpha = \frac{k - 1}{(m, k - 1)}$).
Proof: If \( m = k - 1 \), then \( \beta = \varepsilon(k) \) since \((k, k - 1) = 1\).

By the remark after Theorem 2.20, there exists a constant \( C = C(m, k) \) such that, for every \( t > C \), a \( \text{GD}(\beta t + 1, k - 1, k) \) exists.

By Theorem 1.10 with \( K = \{k\} \), there exists a constant \( C' = C'(k) \) such that for every \( t' > C' \), a \( (k(k-1)t'+1,k,1) \)-BIBD exists.

By deleting one point from this BIBD as mentioned at the beginning of §1.3, we have a \( \text{GD}(kt', k - 1, k) \). Thus \( \alpha \mid (kt' - 1, \beta t) \).

Now choose \( t > \max(C, C') \). Put \( t' = \frac{\beta t}{k} \). Then \( t' = 2t \) or \( t \) depending upon whether \( k \) is odd or even. Thus, \( \alpha \mid (\beta t - 1, \beta t) = 1 \). That is, \( \alpha = 1 \).

Thus, there exists a constant \( N_1 = N(k) \) such that \( \text{GD}(n, k - 1, k) \) exists for every \( n > N_1 \) satisfying \( n(n - 1) \equiv 0 \pmod{k} \).

**Contraction of Groups.**

Let \( m, n, \lambda \in N \) be given such that a \( \text{GD}(n, m, k, \lambda) \) exists. Assume that \((X, \mathcal{B}, \mathcal{C})\) is such a GDD where \( X = I_m \times I_n \), and \( \mathcal{B} = \{I_m \times [i] \mid i \in I_n\} \). Now assume that \( m = ab \) for \( a, b \in N \).

We can partition \( I_m = \bigcup_{s=1}^{b} H_s \) where \( |H_s| = a \) and \( H_s \cap H_t = \emptyset \) for \( s \neq t \in I_b \).

We "contract" \( H_s \) to \([s]\). Then we have that \( Y = I_b \times I_n \), \( \mathcal{H} = \{I_b \times [i] \mid i \in I_n\} \), and \((Y, \mathcal{H}, \mathcal{C}')\) is a \( \text{GD}(n, b, k, \lambda a^2) \).
for some $\alpha'$. In fact, if $B$ is a block of $\sigma$ and $(u,i) \in B$, then we replace $u$ by the index $s$ such that $u \in H_s$ in the partition of $I_m = \bigcup_{s=1}^{b} H_s$, and obtain the block $B'$ of $\sigma'$.

We shall refer to this technique as the 'contraction' of the groups in $\mathcal{S}$ of GDD $(X,\mathcal{S},\mathcal{A})$ by the factor $a$.

Let us observe a very elementary fact. Suppose that $(X,\mathcal{S},\mathcal{A}_1)$ is a GD$(n,m,k,\lambda_1)$ and $(X,\mathcal{S},\mathcal{A}_2)$ is a GD$(n,m,k,\lambda_2)$. For any $a,b \in \mathbb{N}$, we may derive a GD$(n,m,k,a\lambda_1+b\lambda_2)$ by taking the blocks of $\mathcal{A}_1$, each $a$ times, and the blocks of $\mathcal{A}_2$, each $b$ times.

We will use this fact in the proof of the following proposition.

**Proposition 3.7.** Let $k \in \mathbb{N}$ be a given odd integer such that $k - 1 = 2^r \cdot u$ for some $r,u \in \mathbb{N}$ where $u$ is odd. If $m = 2^r$, then $\alpha = u$ (i.e. $\alpha = \frac{k - 1}{(m,k - 1)}$).

**Proof:** By assumption, we have $\beta = 2ku$. By Lemma 3.4, $\alpha|(\beta,k - 1) = 2u$. Equation (2.4), with $K = \{k\}$, implies that $u|\alpha$. It remains to show that $\alpha$ is odd. In order to do this, we need only to exhibit a GD$(n,2^r,k)$ where $n$ is an even integer.

Since $1 \in NG[2^r,k]$, there exists, by Theorem 2.20, a constant $N_0$ such that if $n > N_0$ and $n \equiv 1 \pmod{\beta}$, then $n \in NG[2^r,k]$. Hence we can find an odd integer $t_0$ such that $\beta t_0 + 1 > N_0$ and, hence, $\beta t_0 + 1 \in NG[2^r,k]$.

Observe that since $k$ is odd, the relation $n(n - 1) \equiv 0 \pmod{2k}$ is equivalent to the relation $n(n - 1) \equiv 0 \pmod{k}$. 
By Proposition 3.6, $\alpha(k - 1, k) = 1$. By Theorem 2.5, there exists a constant $N_1$ such that if $n > N_1$ and satisfies $n(n - 1) \equiv 0 \pmod{k}$, then $n \in NG[k - 1, k]$.

By Theorem 1.5, there exists a constant $N_2$ such that if $n > N_2$ and satisfies (1.3) and (1.4), then an $(n, \beta t_0 + 1, 2)$-BIBD exists. Since $(\kappa t_0, \beta t_0 + 1) = 1$, the congruence $s(\kappa t_0) \equiv -1 \pmod{\beta t_0 + 1}$ is solvable in $s$. We can add an odd multiple of $\beta t_0 + 1$ if necessary and obtain a solution $s$ of the congruence such that $s$ is an odd positive integer and $s(\kappa t_0) + 1 > \max(N_1, N_2)$.

Let $n = \kappa t_0 + 1$. Then $n$ is even. Since $\beta = 2\kappa u$,

$$2n(n - 1) \equiv 0 \pmod{(\beta t_0 + 1)\beta t_0} \quad \text{and} \quad 2(n - 1) \equiv 0 \pmod{\beta t_0}$$

Because $n > N_2$, we see that an $(n, \beta t_0 + 1, 2)$-BIBD exists by what we just observed. By Corollary 1.20 with $m = 2^r$, $K = \{k\}$, $\lambda = 1$ and $\lambda' = 2$, we obtain that $n \in NG[2^r, k, 2]$, i.e. a GD$(n, 2^r, k, 2)$ exists. We may assume that $(Y, \mathcal{A}_1)$ is such a GDD where $Y = I_{2^r} \times I_n$ and $\mathcal{A}_1 = \{I_{2^r} \times \{i\} | i \in I_n\}$.

Since $n > N_2$ and $n(n - 1) \equiv 0 \pmod{k}$, a GD$(n, k - 1, k)$ exists, by what we just observed. Assume that $(X, \mathcal{A}_2)$ is such a GDD where $X = I_{k - 1} \times I_n$ and $\mathcal{A}_2 = \{I_{k - 1} \times \{i\} | i \in I_n\}$.

Now do the 'contraction' of the groups of $\mathcal{A}_2$ of the GDD
(X, &_2, G_2) by the factor u (remember that k - 1 = 2^r • u).

Thus, the resulting GDD \((Y, &_1, G_1')\) is a \(GD(n, 2^r, k, u^2)\). Hence we have a \(GD(n, 2^r, k, au^2 + 2b)\) for any \(a, b \in N\). In particular, a \(GD(n, 2^r, k, au^2 + 2)\) exists for any \(a \in N\).

Since \(u\) is odd, \((u^2, 2) = 1\). By Dirichlet's Theorem (2.16), there exists a \(a \in N\) such that \(p = au^2 + 2\) is a prime number and \(p > \beta\). Thus, \(p\) is a unit modulo \(\beta\). Hence there exists a \(f \in N\) such that \(p^f \equiv 1 \pmod{\beta}\). Choose a \(d\) such that \(d\) is a multiple of \(f\), \(d > n^2\), and \(p^d > N\). By Theorem 3.3, a \(GD(n, 2^r p^d, k)\) exists. But \(p^d = 1 \pmod{\beta}\) and \(p^d > N\). Thus, a \(GD(p^d, 2^r, k)\) exists. Using Lemma 1.17 with \(v = n2^r p^d\), \(K = [k]\), \(\lambda' = \lambda = 1\), \(M' = (2^r p^d)\), and \(M = [2^r]\), we have \(n2^r p^d \in G[k][2^r]\), i.e. \(n p^d \in NG[2^r, k]\).

Thus \(\alpha | np^d - 1\). Since \(n\) is even, \(np^d - 1\) is odd. Hence \(\alpha\) is odd, as claimed.

Now we are ready to prove

**Theorem 3.8.** \(\alpha(NG[m, k]) = \frac{k - 1}{(m, k - 1)}\).

**Proof:** If \(m\) is odd, then \(\frac{k(k - 1)}{(m^2, k)(m, k - 1)}\) is even since \(k(k - 1)\) is even. Thus \(\beta = \frac{k(k - 1)}{(m^2, k)(m, k - 1)}\). By Lemma 3.5,

\[
\alpha = \frac{k - 1}{(m, k - 1)}.
\]

Now assume that \(m\) is even. We have 2 cases to discuss.
Case 1. k is even. Thus k - 1 is odd and, hence,

\[
(k - 1, \frac{2k(k - 1)}{(m^2, k)(m, k - 1)}) = (k - 1, \frac{k(k - 1)}{(m^2, k)(m, k - 1)})
\]

\[
= \frac{k - 1}{(m, k - 1)}, \text{ since } (k, k - 1) = 1.
\]

Therefore, by Lemma 3.4, \(\alpha | (\beta, k - 1) = \frac{k - 1}{(m, k - 1)}\). Equation (2.4)

implies that \(\frac{k - 1}{(m, k - 1)} | \alpha\) and, hence \(\alpha = \frac{k - 1}{(m, k - 1)}\), as claimed.

Case 2. k is odd. If \(\frac{k(k - 1)}{(m^2, k)(m, k - 1)}\) is even, then, by

Lemma 3.5, we have the result. Hence we may assume that

\[
\beta = \frac{2k(k - 1)}{(m^2, k)(m, k - 1)}.
\]

Now k - 1 is even. Let \(k - 1 = 2^r \cdot u\)

where u is odd. Since m and k - 1 are even, and

\[
\frac{k(k - 1)}{(m^2, k)(m, k - 1)} \text{ is odd, } \frac{k - 1}{(m, k - 1)} \text{ is odd. Let } m = 2^s \cdot w
\]

where w is odd. Then \(s \geq r\).

Lemma 3.4 implies that \(\alpha | (\beta, k - 1) = \frac{2(k - 1)}{(m, k - 1)}\). Equation

(2.4) implies that \(\frac{k - 1}{(m, k - 1)} | \alpha\). It remains to show that \(\alpha\) is

odd. The construction in Proposition 3.7 shows that there exists

a 'large' even integer \(n\) such that a GD(n, 2^r, k) exists, i.e.

\(n \in NG[2^r, k]\). By Theorem 2.20, there exists a constant

\(N_0(m, k) = N_0\) such that if \(t \in \mathbb{N}\) and \(\beta t + 1 > N_0\), then

\(\beta t + 1 \in NG[m, k]\). Now choose a \(t \in \mathbb{N}\) such that \(\beta t + 1 > N_0\) and
\[ 2^{s-T}(\beta t + 1) \cdot w > o(a(k)) \] where \( o(a(k)) \) is the smallest integer such that if \( s > o(a(k)) \), then \( GD(k,s,k) \) exists. Thus we have \( \beta t + 1 \in NG[m,k] \) and \( GD(k,2^{s-T}(\beta t + 1)w,k) \) exists, i.e. \( k \in NG[2^{s-T}(\beta t + 1)w,k] \). Using Corollary 1.19 with \( m_1 = 2^s \), \( m_2 = 2^{s-T}(\beta t + 1)w, \lambda_1 = \lambda_2 = 1, \) and \( K = [k] \), we see that \( n \in NG[2^w(\beta t + 1),k] = NG[m(\beta t + 1),k] \). Since \( \beta t + 1 \in NG[m,k] \), we have \( mn(\beta t + 1) \in G[k][m] \), by using Lemma 1.17 with \( v = mn(\beta t + 1), M' = [m(\beta t + 1)], M = [m], K = [k], \) and \( \lambda = \lambda' = 1 \). That is, \( n(\beta t + 1) \in NG[m,k] \).

Since \( n \) is even, \( n(\beta t + 1) \) is even. Hence \( \alpha \mid n(\beta t + 1) - 1 \) which is odd. Therefore, \( \alpha \) is odd and we have \( \alpha = \frac{k - 1}{(m,k - 1)} \), as desired.

Therefore, by Theorems 2.18 and 3.8, Theorem 2.4 is proved for the case \( K = [k] \).

\[ \text{§ 3.3 } \alpha(NG[m,K]). \text{ In this section, we will show that} \]
\[ \alpha(NG[m,K]) = \frac{\alpha(K)}{(m,\alpha(K))} \] for given \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \). First, let us observe

**Lemma 3.9.** Let \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Let \( S = \{ \frac{k - 1}{(m,k - 1)} \mid k \in K \} \). Then \( \frac{\alpha(K)}{(m,\alpha(K))} = \gcd(S) \).

**Proof:** Let \( t = \gcd(S) \). By the definition of \( \alpha(k) \), \( \alpha(k) \mid k - 1 \) for every \( k \in K \). Let \( k - 1 = \alpha(k) \cdot u_k \) for some \( u_k \in \mathbb{N} \). Note the fact that if \( a, b, c \in \mathbb{N} \) and \( (a,b) = 1 \), then \( (a,bc) = (a,c) \).
Now, for every \( k \in K \),

\[
(m, k - 1) = (m, \alpha(K) \cdot u_k) \\
= (m, \alpha(K)) \left(\frac{m}{(m, \alpha(K))}, \frac{\alpha(K)}{(m, \alpha(K))} \cdot u_k\right) \\
= (m, \alpha(K)) \left(\frac{m}{(m, \alpha(K))}, u_k\right), \text{ since} \\
\left(\frac{m}{(m, \alpha(K))}, \frac{\alpha(K)}{(m, \alpha(K))}\right) = 1.
\]

So,

\[
\frac{k - 1}{(m, k - 1)} = \frac{\alpha(K) \cdot u_k}{(m, \alpha(K)) \left(\frac{m}{(m, \alpha(K))}, u_k\right)}, \text{ for every } k \in K
\]

Since \( \frac{\alpha(K)}{(m, \alpha(K))} \) and \( \frac{u_k}{(m, \alpha(K))} \) are integers,

\[
\frac{\alpha(K)}{(m, \alpha(K))} \mid \frac{k - 1}{(m, k - 1)} \text{ for every } k \in K. \text{ Thus } \frac{\alpha(K)}{(m, \alpha(K))} \mid t = \gcd(S).
\]

Conversely, let \( d \in \mathbb{N} \) be such that \( d \mid \frac{k - 1}{(m, k - 1)} \) for every \( k \in K \). Since \((m, \alpha(K)) \mid (m, k - 1)\) for every \( k \in K \),

\[
\frac{k - 1}{(m, k - 1)} \mid \frac{k - 1}{(m, \alpha(K))} \text{ for every } k \in K. \text{ Thus } d \mid \frac{k - 1}{(m, \alpha(K))} \text{ for every } k \in K. \text{ Hence } d \mid \frac{\alpha(K)}{(m, \alpha(K))} \text{ by the definition of } \alpha(K).
\]

Therefore \( \frac{\alpha(K)}{(m, \alpha(K))} = \gcd(S) \).

Now we can prove the following result.
Theorem 3.10. Let \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Then
\[
\alpha(NG[m,K]) = \overline{\alpha}(m,K) \quad \text{(i.e.} \quad \alpha(NG[m,K]) = \frac{\alpha(K)}{(m,\alpha(K))}) \quad \text{.}
\]

Proof: Equation (2.4) implies that \( \overline{\alpha}(m,K) \mid n - 1 \) for all \( n \in NG[m,K] \). Hence \( \overline{\alpha}(m,K) \mid \alpha(NG[m,K]) \), by the definition of \( \alpha \).

For every \( k \in K \), we have that \( NG[m,k] \subseteq NG[m,K] \). So,
\[
\alpha(NG[m,K]) \mid \alpha(NG[m,k]) = \frac{k - 1}{(m,k - 1)} \quad \text{by Theorem 3.8, for every} \quad k \in K.
\]

By Lemma 3.9, \( \alpha(NG[m,K]) \mid gcd\left(\frac{k - 1}{(m,k - 1)} \mid k \in K\right) = \frac{\alpha(K)}{(m,\alpha(K))} = \alpha(m,K) \). Therefore, \( \alpha(NG[m,K]) = \overline{\alpha}(m,K) \).

In view of Theorems 2.18 and 3.10, the proof of Theorem 2.4 is now completed by Theorem 2.5.

§3.4 Existence of \( GD(n,m,K,\lambda) \). In this section, we will prove one of our main results, namely,

Theorem 3.11. Let \( m,\lambda \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Then there exists a constant \( N = N(m,K,\lambda) \) such that, if \( n > N \) and satisfies (1.7) and (1.8), then \( n \in NG[m,K,\lambda] \).

First of all, let us observe

Proposition 3.12. Let \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Let \( \lambda \in \mathbb{N} \) be given such that \( \lambda = \sum_{j=1}^{s} a_j \lambda_j \) where \( a_j \geq 0, \lambda_j \geq 1, \quad i = 1, 2, \ldots, s \). Then
\[
\bigcap_{j=1}^{s} \text{NG}[m,K,\lambda_j] \subseteq \text{NG}[m,K,\lambda].
\]

**Proof:** Let \( n \in \bigcap_{j=1}^{s} \text{NG}[m,K,\lambda_j] \). Then there exists a \( \text{GD}(n,m,K,\lambda_j) \), say \((X,\mathcal{A}_j)\), for every \( j \in I_s \). Take all the blocks of \( \mathcal{A}_1 \), each \( a_1 \) times, all the blocks of \( \mathcal{A}_2 \), each \( a_2 \) times, and so on (i.e., take \( a_1 \mathcal{A}_1 + a_2 \mathcal{A}_2 + \ldots + a_s \mathcal{A}_s \)). Let the family so formed by denoted by \( \mathcal{A} \). Then \((X,\mathcal{A})\) is a \( \text{GD}(n,M,K,\lambda) \), i.e. \( n \in \text{NG}[m,K,\lambda] \).

**Corollary 3.13.** Let \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. If \( \lambda, \lambda_0 \in \mathbb{N} \) be given such that \( \lambda_0 | \lambda \), then \( \text{NG}[m,K,\lambda_0] \subseteq \text{NG}[m,K,\lambda] \).

Let \( \lambda, m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Let \( \lambda_0 = (\lambda,\beta(K)) \). Then \( \lambda_0 = (\lambda_0,\beta(K)) \). Since \( \alpha(K) | \beta(K) \), \( \langle \alpha(K) \rangle = \langle \lambda_0, \alpha(K) \rangle \). Therefore (1.7) and (1.8) are equivalent to \( \lambda_0 m^2 n(n - 1) \equiv 0 \pmod{\beta(K)} \) and \( \lambda_0 m(n - 1) \equiv 0 \pmod{\alpha(K)} \), since \( \lambda \) can be written as \( \lambda = b \) where \( b \in \mathbb{N} \) and \( (b,\beta(K)) = 1 = (b,\alpha(K)) \).

Given \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \), if Theorem 3.11 is true for \( \lambda_0 \), then it is true for \( \lambda \) since \( \text{NG}[m,K,\lambda_0] \subseteq \text{NG}[m,K,\lambda] \). Therefore, with given \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \), Theorem 3.11 is true for all \( \lambda \in \mathbb{N} \) iff it is true for those \( \lambda \in \mathbb{N} \) which divides \( \beta(K) \). In particular, if Theorem 3.11 is true, then the constant \( N(m,K,\lambda) \) can be chosen to depend only on \( m \) and \( K \), and not on \( \lambda \). Thus, Theorem 3.11 can be rephrased as
Theorem 3.11'. Given positive integers $m$ and $\lambda$, and a set $K$ of positive integers, there exists a constant $N = N(m,K)$ such that if $n > N$ is a positive integer and satisfies

$$\lambda(n - 1)m \equiv 0 \pmod{\alpha(K)} \quad (1.7)$$

and

$$\lambda n(n - 1)m^2 \equiv 0 \pmod{\beta(K)}, \quad (1.8)$$

then a GD$(n,m,K,\lambda)$ exists.

Recall that $\overline{\beta}(m,K) = \beta(NG[m,K])$ and $\overline{\alpha}(m,K) = \alpha(NG[m,K])$.

Proposition 3.14. Let $m, \lambda \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Then (1.7) and (1.8) are equivalent to

$$n(n - 1) \equiv 0 \pmod{\epsilon \frac{\overline{\beta}(m,K)}{\lambda, \overline{\beta}(m,K)}} \quad (3.7)$$

$$n - 1 \equiv 0 \pmod{\frac{\overline{\alpha}(m,K)}{\lambda, \overline{\alpha}(m,K)}}, \quad (3.8)$$

where $\epsilon$ is defined as in §2.1.

Proof: First of all, we show that (1.7) and (1.8) are equivalent to

$$\lambda n(n - 1) \equiv 0 \pmod{\overline{\beta}(m,K)}, \quad (3.9)$$
\( \lambda(n - 1) \equiv 0 \pmod{\alpha(m, K)}. \)  \hspace{1em} (3.10)

Clearly, (1.7) is equivalent to (3.10). Now assume (1.7) and (1.8). But (1.8) implies that \( \lambda(n - 1)m^2 \equiv 0 \pmod{\gamma(K)} \) since \( \beta(K) = \alpha(K)\gamma(K) \). Hence,

\[ \lambda(n - 1) \equiv 0 \pmod{\frac{\gamma(K)}{(m^2, \gamma(K))}}. \]

Since \( (\alpha(K)), \gamma(K)) = 1 \), \( \left( \frac{\alpha(K)}{(m, \alpha(K))}, \frac{\gamma(K)}{(m^2, \gamma(K))} \right) = 1 \). Thus,

\[ \lambda(n - 1) \equiv 0 \pmod{\beta(m, K)}, \]

since \( n(n - 1) \) is even.

Conversely, let us assume (3.9) and (3.10). But (3.9) implies that

\[ \frac{\beta(K)}{(m^2, \gamma(K))(m, \alpha(K))} \cdot m^2 | \lambda(n - 1)m^2. \]

Now \( (m^2, \gamma(K)) \) and \( (m, \alpha(K)) \) are relatively prime, and both divide \( m^2 \). Hence,

\[ \beta(K) \cdot \frac{m^2}{(m^2, \gamma(K))(m, \alpha(K))} | \lambda(n - 1)m^2, \]

i.e. (1.7) is valid. Thus, (1.7) and (1.8) are equivalent to (3.9) and (3.10) which are, in turn, equivalent to (3.7) and (3.8),
since $n(n - 1)$ is even.

Thus, Theorem 3.11' can be rephrased as

**Theorem 3.11'.** Let $m, \lambda \in \mathbb{N}$ and $K \subset \mathbb{N}$ be given. Then there exists a constant $N = N(m, K)$ such that if $n > N$ and satisfies (3.7) and (3.8), then $n \in \mathbb{N}G[m, K, \lambda]$.

By Corollary 1.21, $\mathbb{N}G[m, K, \lambda]$ is closed. In order to prove Theorem 3.11", it is sufficient, by Theorem 1.10, to show that

$$\beta(\mathbb{N}G[m, K, \lambda]) = \varepsilon \left( \frac{\bar{\beta}(m, K)}{(\lambda, \bar{\beta}(m, K))} \right)$$

and

$$\alpha(\mathbb{N}G[m, K, \lambda]) = \frac{\bar{\alpha}(m, K)}{(\lambda, \bar{\alpha}(m, K))}.$$  

In the course of the proof of (3.11) and (3.12), we will use one of the propositions in [27]. We now state it without proof.

(For proof, see Proposition 9.2 in [27], p. 226.)

**Proposition 3.15.** Let $\lambda \in \mathbb{N}$ and $K \subset \mathbb{N}$ be given. Then

$$\beta(B[K; \lambda]) = \varepsilon \left( \frac{\bar{\beta}(K)}{(\lambda, \bar{\beta}(K))} \right) \quad \text{and} \quad \alpha(B[K; \lambda]) = \frac{\bar{\alpha}(K)}{(\lambda, \bar{\alpha}(K))},$$

where $\varepsilon$ is defined as in §2.1.

**Proof of (3.11):** By (3.7), $\varepsilon \left( \frac{\bar{\beta}(m, K)}{(\lambda, \bar{\beta}(m, K))} \right)n(n - 1)$ for
every \( n \in NG[m,K,\lambda] \). Thus \( \epsilon\left(\frac{-\beta(m,K)}{\lambda,\beta(m,K)}\right) |\beta(NG[m,K,\lambda]) \), by the definition of \( \beta \).

By Corollary 1.22, \( B[NG[m,K];\lambda] \subseteq NG[m,K,\lambda] \). Hence, we have

\[
\beta(NG[m,K,\lambda]) |\beta(B[NG[m,K];\lambda]) = \epsilon\left(\frac{-\beta(m,K)}{\lambda,\beta(m,K)}\right),
\]

by Proposition 3.15 and the fact that \( \beta(NG[m,K]) = \beta(m,K) \).

Therefore, (3.11) is established.

Proof of (3.12). By Proposition 3.14, \( \frac{\alpha(m,K)}{\lambda,\alpha(m,K)} |(n - 1) \) for every \( n \in NG[m,K,\lambda] \). Hence \( \frac{\alpha(m,K)}{\lambda,\alpha(m,K)} |\alpha(NG[m,K,\lambda]) \).

By Corollary 1.22, \( B[NG[m,K];\lambda] \subseteq NG[m,K,\lambda] \). Hence,

\[
\alpha(NG[m,K,\lambda]) |\alpha(B[NG[m,K];\lambda]) = \frac{\alpha(m,K)}{\lambda,\alpha(m,K)},
\]

by Proposition 3.15 and the fact that \( \alpha(NG[m,K]) = \alpha(m,K) \).

Therefore, (3.12) is shown.

From these, the proof of Theorem 3.11" (hence, Theorems 3.11 and 3.11'') is now complete.

§3.5 Existence of GD(n,m,3). In this section, we will prove that, for \( K = [3] \) and \( \lambda = 1 \), the constant \( N \) in Theorem 3.11 can be replaced by 0, i.e.

Theorem 3.16. Let \( m \in \mathbb{N} \). The necessary and sufficient conditions for the existence of a GD(n,m,3) are
\[ n(n - 1)m^2 \equiv 0 \pmod{6} \]  \hspace{1cm} (3.13)

and

\[ (n - 1)m \equiv 0 \pmod{2} \]  \hspace{1cm} (3.14)

As we mentioned in §1.2, an \((n,3,1)\) - BIBD exists for a given positive integer \(n\) iff \(n = 1\) or \(3 \pmod{6}\) (see [20] and [24]).

**Lemma 3.17.** \(3 \in \text{NG}[m,3]\) for every \(m \in \mathbb{N}\).

**Proof:** It is well known [10] that a \(\text{GD}(k,m,k)\) exists iff there exists \(k - 2\) mutually orthogonal Latin squares of order \(m\). Now \(k = 3\) and there is a Latin square of order \(m\) for every \(m \in \mathbb{N}\). Hence \(\text{GD}(3,m,3)\) exists for every \(m \in \mathbb{N}\), i.e. \(3 \in \text{NG}[m,3]\).

**Lemma 3.18.** \(\{4,6\} \subseteq \text{NG}[m,3]\) if \(m\) is even.

**Proof:** It is well known that \((9,3,1)\) - BIBD and \((13,3,1)\) - BIBD exist. Take a \((9,3,1)\) - BIBD and delete one point from it. As we observed in §1.3, we will get a \(\text{GD}(4,2,3)\), say \((X,\mathcal{A})\). Let \(w: X \to \mathbb{N}\) be a weighting such that \(w(x) = \frac{m}{2}\) for \(x \in X\). For each block \(B\) of \(\mathcal{A}\), there is a \(\text{GD}(3,m/2,3)\), by Lemma 3.17. By Theorem 1.18, we have a \(\text{GD}(4,m,3)\), i.e. \(4 \in \text{NG}[m,3]\). Take a \((13,3,1)\) - BIBD. Proceed as before and obtain \(6 \in \text{NG}[m,3]\).

A BIBD \((X,\mathcal{A})\) is resolvable if \(\mathcal{A}\) can be partitioned into parallel classes of blocks. A resolvable \((n,3,1)\) - BIBD is called a Kirkman design. It is proved [22] that a Kirkman design on \(n\) points exists iff \(n \equiv 3 \pmod{6}\).
Lemma 3.19. If \( n \geq 3 \) and \( n \equiv 0 \) or \( 1 \) (mod 3), then \( n \in B[3,4,6] \).

Proof: If \( n \equiv 1 \) or \( 3 \) (mod 6), then \( n \in B[3] \subseteq B[3,4,6] \). Hence we may assume from now on that \( n \equiv 0 \) or \( 4 \) (mod 6).

Case 1. \( n \equiv 0 \) (mod 6). Let \( n = 6t \) for \( t \in \mathbb{N} \). Then \( t \geq 1 \). If \( t = 1 \), then \( n = 6 \in B[3,4,6] \). So, we assume that \( t \geq 2 \). Now let \( s = 6t - 3 \). Then \( s \equiv 3 \) (mod 6). Hence a Kirkman design on \( s \) points exists, say \((X,d)\). The number of parallel classes of blocks is \( 3t - 2 \). Let \( \mathcal{A} = \bigcup_{i=1}^{3t-2} \mathcal{A}_i \) be the partition of \( \mathcal{A} \) into parallel classes. Since \( t \geq 2 \), we have at least 4 parallel classes. Choose 3 of them, say \( \mathcal{A}_1, \mathcal{A}_2 \) and \( \mathcal{A}_3 \). Let \( Y = \{o_1, o_2, o_3\} \) be such that \( X \cap Y = \emptyset \). Let \( X^* = X \cup Y \), \( B^* = B \cup \{o_1\} \) for each \( B \in \mathcal{A}_i \), \( i = 1, 2, 3 \). Now let

\[
\mathcal{A}_i = \{B^* \mid B \in \mathcal{A}_i\}, \quad i = 1, 2, 3, \text{ and }
\]

\[
\mathcal{A}^* = \mathcal{A}_1^* \cup \mathcal{A}_2^* \cup \mathcal{A}_3^* \cup \left( \bigcup_{i=4}^{3t-2} \mathcal{A}_i \right) \cup \{o_1, o_2, o_3\}
\]

as the set of blocks. Then, obviously, \((X^*,\mathcal{A}^*)\) is an \((n, [3,4], 1)\)-PBD, i.e. \( n \in B[3,4,6] \).

Case 2. \( n \equiv 4 \) (mod 6). Let \( n = 6t + 4 \) for \( t \in \mathbb{N}_0 \). If \( t = 0 \), then \( 4 \in B[3,4,6] \). Hence, assume \( t \geq 1 \). There exists a Kirkman design on \( 6t + 3 \) points, say \((X,d)\). The number of
parallel classes of blocks is $3t + 1$. Let $\mathcal{a} = \bigcup_{i=1}^{3t+1} \mathcal{a}_i$ be the partition of $\mathcal{a}$ into parallel classes. Let $\emptyset$ be a new element, not in $X$. Let $X^* = X \cup \{\emptyset\}$, $B^* = B \cup \{\emptyset\}$ for each $B \in \mathcal{a}_1$, and $\mathcal{a}_1^* = \{B^* \mid B \in \mathcal{a}_1\}$. Let $\mathcal{a}^* = \mathcal{a}_1^* \cup \bigcup_{i=2}^{3t+1} \mathcal{a}_i$.

Then, as before, $(X^*, \mathcal{a}^*)$ is an $(n, \{3, 4\}, 1)$-PBD, i.e. $n \in \mathcal{B}([3, 4, 6])$.

**Proposition 3.20.** Given $m \in \mathbb{N}$ such that $m$ is even and $3 \nmid m$. Then $n \in \mathcal{N}[m, 3]$ iff $n \equiv 0$ or $1 \pmod{3}$.

**Proof:** Necessity is clear. Assume that $n \equiv 0$ or $1 \pmod{3}$. By Lemma 3.19, $n \in \mathcal{B}([3, 4, 6])$. By Lemmas 3.17 and 3.18, $3, 4, 6 \in \mathcal{N}[m, 3]$. Therefore, we have that $n \in \mathcal{B}([3, 4, 6]) \subseteq \mathcal{B}[\mathcal{N}[m, 3]] = \mathcal{N}[m, 3]$.

**Proposition 3.21.** Given $m \in \mathbb{N}$ such that $m$ is odd and $3 \nmid m$. Then $n \in \mathcal{N}[m, 3]$ iff $n \equiv 1$ or $3 \pmod{6}$.

**Proof:** Necessity is clear. If $n \equiv 1$ or $3 \pmod{6}$, then $n \in \mathcal{B}[3]$. By Lemma 3.17, $3 \in \mathcal{N}[m, 3]$. Therefore, $n \in \mathcal{B}[3] \subseteq \mathcal{B}[\mathcal{N}[m, 3]] = \mathcal{N}[m, 3]$.

**Proposition 3.22.** Given $m \in \mathbb{N}$ such that $m$ is odd and $3 \mid m$. Then, for $n \geq 3$, $n \in \mathcal{N}[m, 3]$ iff $n$ is odd.

**Proof:** Necessity is clear. Conversely, let $n = 2s + 1$ and $m = 3t$ for $s, t \in \mathbb{N}$. Then $t$ is odd. There is a Kirkman design
on \( 3(2s + 1) = 6s + 3 \) points, say \((X, \mathcal{A})\). Let \( \mathcal{A}_1 \subseteq \mathcal{A} \) be one of the parallel classes of \( \mathcal{A} \). Let \( \mathcal{A}' = \mathcal{A} \setminus \mathcal{A}_1 \). Then \((X, \mathcal{A}_1, \mathcal{A}')\) is a GD\((2s + 1, 3, 3)\). Let \( w: X \to N \) be a weighting such that \( w(x) = t \) for every \( x \in X \). Now, for each block \( B \) of \( \mathcal{A}' \), a GD\((3, t, 3)\) exists by Lemma 3.17. By Theorem 1.18, a GD\((n, m, 3)\) exists, i.e. \( n \in NG[m, 3] \).

**Proposition 3.23.** Given \( m \in N \) such that \( m \equiv 0 \pmod{6} \). Then \( n \in NG[m, 3] \) for all positive integers \( n \geq 3 \).

**Proof:** Let \( m = 6t \) for some \( t \in N \). If \( n \) is odd, then we use the same argument as in Proposition 3.22 with the weighting \( w: X \to N \) defined by \( w(x) = 2t \) for every \( x \in X \) and the existence of GD\((3, 2t, 3)\) by Lemma 3.17. So, assume, from now on, that \( n \) is even.

**Case 1.** \( n \equiv 0 \text{ or } 1 \pmod{3} \). Then \( 2n + 1 \equiv 1 \text{ or } 3 \pmod{6} \). There is a \((2n + 1, 3, 1)\)-BIBD. Delete one point from this BIBD and we obtain, as in §1.3, a GD\((n, 2, 3)\), say \((X, \mathcal{A}_1, \mathcal{A})\). Let \( w: X \to N \) be a weighting defined by \( w(x) = 3t \) for every \( x \in X \). By Lemma 3.17, a GD\((3, 3t, 3)\) exists. By Theorem 1.18, a GD\((n, m, 3)\) exists, i.e. \( n \in NG[m, 3] \).

**Case 2.** \( n \equiv 2 \pmod{3} \). Hanani showed [16] that, for every \( n \geq 3, n \in B[3, 4, 5, 6, 8] \). By Lemmas 3.17 and 3.18, \( 3, 4, 6 \in NG[m, 3] \) since \( m \) is even. There is a Kirkman design on 15 points. Take one parallel class of blocks and treat them as groups. Then we have
a GD(5,3,3), i.e. \(5 \in \text{NG}[m,3]\).

By an affine plane of order \(n\), AG(n), we mean a \((n^2,n,1)\)-BIBD. It has been proved [7] that AG(n) exists whenever \(n\) is a prime power. Now consider AG(7). Then it is a \((49,7,1)\)-BIBD. Deleting one point from it, we obtain a GD(8,6,7), say \((X,Jr,tf)\). For each block \(B\) of \(\mathcal{A}\), there is a \((7,3,1)\)-BIBD. By Lemma 1.16 (breaking up blocks), we obtain a GD(8,6,3). Now let \(w: X \rightarrow \mathbb{N}\) be a weighting such that \(w(x) = t\) for every \(x \in X\). For each block of GD(8,6,3), a GD(3,t,3) exists. By Theorem 1.18, a GD(8,m,3) exists. Therefore \(8 \in \text{NG}[m,3]\).

Hence \([3,4,5,6,8] \subseteq \text{NG}[m,3]\). Therefore, for \(n \geq 3\), \(n \in B[(3,4,5,6,8)] \subseteq B[\text{NG}[m,3]] = \text{NG}[m,3]\), since \text{NG}[m,3] is a closed set.

By Propositions 3.20, 3.21, 3.22, and 3.23, the proof of Theorem 3.16 is now completed. As a concluding remark of this chapter, we have

**Theorem 3.24.** Let \(k \geq 3\) and \(\lambda\) be given positive integers. Then there is \(n_0 = n_0(k,\lambda) \in \mathbb{N}\) with the property:

given \(n > n_0\), there exists a constant \(m_0 = m_0(k)\) such that a GD\((n,m,k,\lambda)\) exists for all \(m > m_0\) satisfying

\[
\lambda n(n - 1)m^2 \equiv 0 \pmod{k(k - 1)} \quad \text{and} \quad (3.15)
\]
\[ \lambda(n - 1)m \equiv 0 \pmod{(k - 1)}. \quad (3.16) \]

**Proof:** Let \( D = \{ d \in \mathbb{N} \mid d \text{ is a divisor of } k(k - 1) \} \).

By Theorem 3.11, there is a positive integer \( n_d = n(d,k,\lambda) \) such that \( GD(n_d,k,\lambda) \) exists for all \( n > n_d \) satisfying (3.15) and (3.16). Let \( n_1 = \max\{n_d \mid d \in D\} \). By Theorem 1.5, let \( n_2 \) be the positive integer such that an \((n, k, \lambda)\)-BIBD exists for all \( n > n_2 \) satisfying (1.3) and (1.4). Now let \( n_0 = \max(n_1, n_2) \).

Let \( m_0 = k(k - 1)\alpha(k) \) where \( \alpha(k) \) is the smallest number such that \( GD(k,m,k) \) exists for all \( m > \alpha(k) \). Let \( m > m_0 \) be a given positive integer satisfying (3.15) and (3.16). We have two cases.

**Case 1.** \((m,k(k - 1)) = 1\). Then (3.15) and (3.16) reduce to (1.3) and (1.4). Since \( n > n_0 > n_2 \), an \((n,k,\lambda)\)-BIBD exists, say \((X,\mathscr{A})\). Let \( w: X \to \mathbb{N} \) be a weighting defined by \( w(x) = m \) for every \( x \in X \). Since \( m > m_0 > \alpha(k) \), a \( GD(k,m,k) \) exists. By Theorem 1.18, a \( GD(n,m,k,\lambda) \) exists.

**Case 2.** \((m,k(k - 1)) = d \neq 1\). Then (3.15) and (3.16) reduce to

\[ \lambda n(n - 1)d^2 \equiv 0 \pmod{k(k - 1)} \]

and

\[ \lambda(n - 1)d \equiv 0 \pmod{(k - 1)}. \]

Since \( n > n_0 > n_1 > n_d \), a \( GD(n_d,k,\lambda) \) exists, say \((X,\mathscr{A})\).
Let $w : X \rightarrow \mathbb{N}$ be a weighting defined by $w(x) = \frac{m}{d}$ for every $x \in X$. Now, since $\frac{m}{d} > \frac{m}{k(k-1)} > \frac{m^o}{k(k-1)} = o\alpha(k)$, a $GD(k, \frac{m}{d}, k)$ exists. By Theorem 1.18, a $GD(n,m,k,\lambda)$ exists.
\section{Preliminaries.}

In this chapter, we will prove theorems for the existence of LD's. As we remarked in §1.4, an LD\((n,m,K,\lambda)\) exists iff an LD\((m,n,K,\lambda)\) exists by just interchanging the roles of vertical and horizontal groups. Recall the two closed sets (with respect to the closure operation \(\mathcal{B}\)) \(\text{NHG}[m,K,\lambda] = \{n \in \mathbb{N} \mid \text{an LD}(n,m,K,\lambda) \text{ exists}\}\) and \(\text{NVG}[n,K,\lambda] = \{m \in \mathbb{N} \mid \text{an LD}(n,m,K,\lambda) \text{ exists}\}\). From now on, we will restrict our attention to \(\text{NHG}[m,K,\lambda]\). For all the results which we will get for \(\text{NHG}[m,K,\lambda]\), we will have corresponding results for \(\text{NVG}[n,K,\lambda]\). For ease of description, we shall, in the first 5 sections, deal with LD's having index of pairwise balance \(\lambda = 1\). As mentioned in §1.4, we shall denote such an LD by \(\text{LD}(n,m,K)\) and \(\text{NHG}[m,K,1]\) by \(\text{NHG}[m,K]\). Recall the function \(\varepsilon: \mathbb{Z} \rightarrow \mathbb{Z}\) defined in §2.1, namely \(\varepsilon(x) = x\) if \(x\) is even and \(\varepsilon(x) = 2x\) if \(x\) is odd.

We recall Proposition 1.36 and obtain that if \(n \in \text{NHG}[m,K]\), then

\begin{align*}
n(n - 1)m(m - 1) &\equiv 0 \pmod{\beta(K)}, \quad \text{and} \quad (4.1) \\
(n - 1)(m - 1) &\equiv 0 \pmod{\alpha(K)} \quad (4.2)
\end{align*}
By Corollary 1.35, we know that \( \text{NHG}[m,K] \) is a closed set. In view of Theorem 1.10, we first obtain the following proposition.

**Proposition 4.1.** Let \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Then the relations (4.1) and (4.2) are equivalent to the relations

\[
\begin{align*}
    n(n - 1) &\equiv 0 \pmod{\beta^*(m,K)}, \quad \text{and} \\
    (n - 1) &\equiv 0 \pmod{\alpha^*(m,K)} 
\end{align*}
\]

where

\[
\begin{align*}
    \beta^*(m,K) &= e\left(\frac{\beta(K)}{(m(m - 1),\gamma(K))(m - 1,\alpha(K))}\right) \\
    \alpha^*(m,K) &= \frac{\alpha(K)}{(m - 1,\alpha(K))} 
\end{align*}
\]

**Proof:** Clearly, \( (n - 1)(m - 1) \equiv 0 \pmod{\alpha(K)} \) is equivalent to \( n - 1 \equiv 0 \pmod{\alpha^*(m,K)} \). Now assume (4.1) and (4.2). It remains to exhibit (4.3). However, (4.1) implies that

\[
n(n - 1)m(m - 1) \equiv 0 \pmod{\gamma(K)}, \quad \text{since} \quad \beta(K) = \alpha(K)\gamma(K). \quad \text{Hence,}
\]

\[
n(n - 1) \equiv 0 \pmod{\frac{\gamma(K)}{(m(m - 1),\gamma(K))}}.
\]

By Lemma 2.1, \( (\alpha(K),\gamma(K)) = 1 \). Thus, \( \frac{\alpha(K)}{(m - 1,\alpha(K))} \frac{\gamma(K)}{(m(m - 1),\gamma(K))} = 1 \). Further, \( \frac{\alpha(K)}{(m - 1,\alpha(K))} | n - 1 \). Hence we have that
\( n(n - 1) \equiv 0 \pmod{\frac{\beta(K)}{(m(m - 1), \gamma(K))(m - 1, \alpha(K))}}. \)

Since \( n(n - 1) \) is even, \( n(n - 1) \equiv 0 \pmod{\beta^*(m, K)}. \)

Now let us assume (4.3) and (4.4). It remains to exhibit (4.1). (4.3) implies that

\[
\frac{\beta(K)}{(m(m - 1), \gamma(K))(m - 1, \alpha(K))} m(m - 1) | n(n - 1)m(m - 1).
\]

By Lemma 2.1, \((m(m - 1), \gamma(K))\) and \((m - 1, \alpha(K))\) are relatively prime. Further, both of them divide \( m(m - 1) \). Hence,

\[
(m(m - 1), \gamma(K))(m - 1, \alpha(K)) \mid m(m - 1)
\]

and

\[
\frac{\beta(K)m(m - 1)}{(m(m - 1), \gamma(K))(m - 1, \alpha(K))} \mid n(n - 1)m(m - 1).
\]

Thus, \( n(n - 1)m(m - 1) \equiv 0 \pmod{\beta(K)}, \) as desired.

Let \( m \in \mathbb{N} \) be a given positive integer and \( q \) be a given prime power. Let \( X = \mathbb{I}_m \times GF(q) \). Let \( H_u = \mathbb{I}_m \times \{u\} \) for every \( u \in GF(q) \) and \( V_i = \{i\} \times GF(q) \) for every \( i \in \mathbb{I}_m \). Let

\( \mathcal{H} = \{H_u | u \in GF(q)\} \) and \( \mathcal{V} = \{V_i | i \in \mathbb{I}_m\} \). Let \( B \subseteq X \) be a given subset, say

\[
B = \{(l_1, b_1), (l_2, b_2), \ldots, (l_k, b_k)\},
\]

where \( b_i \in GF(q), \ l_i \in \mathbb{I}_m \) for \( i = 1, 2, \ldots, k \). For
a, c ∈ GF(q), recall the definition of aB + c, given in §2.2, namely, aB + c = \{(l_1ab_1 + c)(l_2ab_2 + c), \ldots, (l_kab_k + c)\}.

For every 1 ≤ l_1 < l_2 ≤ m, recall the definition of Δ(B, (l_1, l_2)), given in §2.2, namely, the list of elements of GF(q) which contain an entry u - v for every ordered pair ((l_1v), (l_2u)) of elements of B. If B = \{B_1, B_2, \ldots, B_t\}, let us define, as before, Δ(B, (l_1, l_2)) = \sum_{i=1}^{t} Δ(B_i, (l_1, l_2)). With this terminology in mind, let us observe the following very important fact.

**Proposition 4.2.** Let K ⊆ H be a given subset. Let B = \{B_1, B_2, \ldots, B_t\} be a family of given subsets of X such that |B_i| ∈ K for every i ∈ I, |B_i ∩ H_u| ≤ 1 and |B_i ∩ V_j| ≤ 1 for every i ∈ I, j ∈ I, u, v ∈ GF(q). The quadruple (X, γ, M, \bigcup_{i=1}^{t} \{B_i + c \mid c ∈ GF(q)\}) is an LD(q, m, K) iff

\[ Δ(B, (l_1, l_2)) = GF(q)^* = GF(q) - \{0\} \] (i.e. Δ(B, (l_1, l_2)) contains every nonzero element of GF(q) exactly once), for every 1 ≤ l_1 < l_2 ≤ m.

**Proof:** The necessity of the conditions is clear (by observing the two elements (l_1, 0) and (l_2, x)). To prove sufficiency, let (l_1, b) and (l_2, a) be two distinct elements of X with l_1 ≠ l_2 and a ≠ b. Assume that l_1 < l_2. By assumption, there is a unique \(i_0 \in I\) such that Δ(B_{i_0}, (l_1, l_2)) contains a - b.

Consider the sets \(T = \{c ∈ GF(q) \mid ((l_1, b), (l_2, a)) ∈ B_{i_0} + c\}\) and
Define the mapping \( \varphi: T \rightarrow D \) by \( \varphi(c) = ((l_1, b - c), (l_2, a - c)) \). Then it is easily seen that \( \varphi \) is bijective, i.e. the number of \( c \in GF(q) \) such that \( ((l_1, b), (l_2, a)) \in B_i + c \) is equal to the number of times that \( a - b \) occurs in the list \( \Delta(B_i, (l_1, l_2)) \). Hence there is a unique \( c_0 \in GF(q) \) such that \( ((l_1, b), (l_2, a)) \in B_i + c_0 \).

Remark: We will get an LD\((q, m, K, \lambda)\) if we replace the condition \( \Delta(\mathbb{F}, (l_1, l_2)) = GF(q)^* \) by the condition \( \Delta(\mathbb{F}, (l_1, l_2)) = \lambda \cdot [GF(q)^*] \). The above proposition is still true if we replace the set \( I_m \) by any \( m \)-set \( M \). The modifications to the statement and its proof are easily seen.

Let \( m, e \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) be given. Then we have the following

**Proposition 4.3.** The relations

\[
e m (m - 1) \equiv 0 \pmod{\beta(K)} \quad \text{and} \quad (4.7)
\]
\[
e (m - 1) \equiv 0 \pmod{\alpha(K)} \quad \text{(4.8)}
\]

are equivalent to the relation

\[
e \equiv 0 \pmod{\beta_1^* (m, K)} \quad \text{(4.9)}
\]

where
\[ \beta_1^*(m, K) = \frac{\beta(K)}{(m(m-1), \gamma(K))(m-1, \alpha(K))} \cdot \] (4.10)

Proof: We observe, first of all, that \( e(m-1) \equiv 0 \pmod{\alpha(K)} \) is equivalent to \( e \equiv 0 \pmod{\frac{\alpha(K)}{(m-1, \alpha(K))}} \). Now assume (4.9).

By the definition of \( \beta_1^*(m, K) \), we have, from (4.9) that

\[ \alpha^*(m, K) = \frac{\alpha(K)}{(m-1, \alpha(K))} \mid e, \text{ i.e. } e(m-1) \equiv 0 \pmod{\alpha(K)}. \]

Now \( e \equiv 0 \pmod{\beta_1^*(m, K)} \) implies that, for some \( t \in \mathbb{N} \),

\[ e = t \cdot \frac{\beta(K)}{(m(m-1), \gamma(K))(m-1, \alpha(K))}. \]

Thus,

\[ em(m-1) = t \cdot \frac{\beta(K)}{(m(m-1), \gamma(K))(m-1, \alpha(K))} \cdot m(m-1). \]

Now \( (m(m-1), \gamma(K)) \) and \( (m-1, \alpha(K)) \) are relatively prime and both divide \( m(m-1) \). Hence \( (m(m-1), \gamma(K))(m-1, \alpha(K)) \mid m(m-1) \).

Therefore,

\[ em(m-1) = t \beta(K) \cdot \frac{m(m-1)}{(m(m-1), \gamma(K))(m-1, \alpha(K))}, \]

i.e.

\[ em(m-1) \equiv 0 \pmod{\beta(K)}. \]

Conversely, let us assume (4.7) and (4.8). (4.8) implies that \( \beta_1^*(m, K) = t \beta(K) \) for some \( t \in \mathbb{N} \). Therefore,
\[
e^{-\frac{m(m-1)}{(m(m-1),\gamma(K))}} = t \cdot \frac{\gamma(K)}{(m(m-1),\gamma(K))} \alpha(K).
\]

Now \(\frac{m(m-1)}{(m(m-1),\gamma(K))}\) and \(\frac{\gamma(K)}{(m(m-1),\gamma(K))}\) are relatively prime.

We have

\[
\frac{\gamma(K)}{(m(m-1),\gamma(K))} \mid e.
\]

But (4.8) is equivalent to \(\frac{\alpha(K)}{(m-1,\alpha(K))} \mid e\). Further, \(\frac{\alpha(K)}{(m-1,\alpha(K))}\) and \(\frac{\gamma(K)}{(m(m-1),\gamma(K))}\) are relatively prime. Thus, we have that

\[e \equiv 0 \pmod{\beta_1^*(m,K)}.
\]

Theorem 1.5 can be rephrased as

**Theorem 1.5'.** Let \(K \subseteq \mathbb{N}\) and \(e \in \mathbb{N}\) be given. There exists a constant \(M\) such that \(m \in B[K;e]\) for all \(m > M\) satisfying (4.7) and (4.8).

As remarked in [26] (p. 253), the constant \(M\) can be chosen to be independent of \(e\). Let \(M(K)\) denote the smallest integer for which Theorem 1.5' holds.

Let \(K \subseteq \mathbb{N}\) be given. By Proposition 2.14, there is a finite set \(K_o \subseteq K\) such that \(\beta(K_o) = \beta(K), \alpha(K_o) = \alpha(K),\) and \(\gamma(K_o) = \gamma(K)\). Let
\( C = \{ S \mid S \subseteq K \text{ is a finite set, } \beta(S) = \beta(K), \alpha(S) = \alpha(K), \text{ and } \gamma(S) = \gamma(K) \} \).

For each \( K \in \mathbb{N} \), define \( M_0(K) = \min_{S \in C} M(S) \).

For each \( K \in \mathbb{N} \), pick a finite subset \( K_0 \) of \( K \) such that \( K_0 \subseteq C \) and \( M_0(K) = M(K_0) \). For the purpose of this chapter, we will fix this \( K_0 \) in our consideration. Thus, \( \beta^*(m, K_0) = \beta^*(m, K) \) (in particular, \( \beta^*_1(m, K) = \beta^*_1(m, K_0) \)) and \( \alpha^*(m, K_0) = \alpha^*(m, K) \). Therefore, we have

**Corollary 4.4.** Given \( K \in \mathbb{N} \) and \( e \in \mathbb{N} \), an \((m, K, e)\) - PBD exists for all positive integer \( m > M_0(K) \) satisfying (4.7) and (4.8).

By Proposition 4.3, if an \((m, K, e)\) - PBD exists, then \( e \) must be of the form \( t \beta^*_1(m, K) \) for some \( t \in \mathbb{N} \). Thus, for our purpose of application, we have a corollary of Theorem 1.5:

**Corollary 4.5.** Let \( K \in \mathbb{N} \) be given. Given a positive integer \( m > M_0 = M_0(K) \) (see Corollary 4.4), an \((m, K, t \beta^*_1(m, K))\) - PBD exists for any \( t \in \mathbb{N} \).

If \( K = \{k\} \), then a corollary of the main result in [31] is the following

**Theorem 4.6.** Given positive integers \( m \geq k \), there exists a constant \( E = E(m, k) \) such that an \((m, k, e)\) - BIBD exists for all
Let \( E(m,k) \) be the smallest integer for which Theorem 4.6 holds. By Proposition 4.3 again, we have that if an \((m,k,e)\)-BIBD exists, then \( e \) must be of the form \( t\beta_1^*(m,k) \) for some \( t \in \mathbb{N} \).

Thus, we have, for our purpose of application, a corollary of Theorem 4.6.

**Corollary 4.7.** Given positive integers \( m > k \), there exists a constant \( \tilde{T} = \tilde{T}(m,k) \) such that an \((m,k,t\beta_1^*(m,k))\)-BIBD exists for all \( t > \tilde{T} \).

Let \( \tilde{T}(m,k) \) be the smallest integer for which Corollary 4.7 holds.

§4.2 A Direct Construction of LD's. In this section, we will construct a class of LD's with the aids of Theorem 1.11, Proposition 4.2, and the finite fields. Assume that \( K \subseteq \mathbb{N} \) is a given finite subset. Let \( m,e \in \mathbb{N} \) be given positive integers such that an \((m,K,e)\)-PBBD exists. Assume that \((I_m,\mathfrak{A})\) is such an \((m,K,e)\)-PBBD. Let \( b \in \mathbb{N} \) be the number of blocks in this PBBD. Thus, we may write \( \mathfrak{A} = (B_i \mid i \in I_b) \). Let \( q \in \mathbb{N} \) be a prime power such that \( q = 1 \pmod{e} \) and \( q > e^{\max(K)}(\max(K) - 1) \).

Let \( \omega \in \text{GF}(q) \) be a primitive element of \( \text{GF}(q) \). Recall the cosets modulo the e-th powers of \( \omega \), defined in §1.2,

\[
H_j^e = \{ \omega^t \mid t \equiv j \pmod{e} \}, \quad j = 0, 1, 2, \ldots, e - 1,
\]
and the class of cosets, \( \mathcal{C} = \{ H_0^e, H_1^e, \ldots, H_{e-1}^e \} \).

Let \( X^* = I_m \times GF(q) \). Let \( H_u = I_m \times \{ u \} \) for every \( u \in GF(q) \) and \( V_i = \{ i \} \times GF(q) \) for every \( i \in I_m \). Let \( M = \{ H_u \mid u \in GF(q) \} \) and \( V = \{ V_i \mid i \in I_m \} \). We are now going to construct the blocks.

First of all, let us examine Theorem 1.11 once more. Let \( r = H \). Recall the set \( P(r) = \{ (i, j) \mid 1 < i < j < r \} \) defined in §1.2. Now let \( S \subseteq N \) be any \( r \)-set, say \( S = \{ s_1, s_2, \ldots, s_r \} \) where \( s_1 < s_2 < \ldots < s_r \). Define the set \( P(S) = \{ (s_i, s_j) \mid 1 < i < j < r \} \). It is easily seen that the mapping \( \phi: P(r) \rightarrow P(S) \) defined by \( \phi(i,j) = (s_i, s_j) \) is bijective. Hence, for any choice function \( C: P(S) \rightarrow \mathcal{C} \), \( C \phi: P(r) \rightarrow \mathcal{C} \) is also a choice function. By Theorem 1.11, there exists an \( r \)-tuple \( (a_1, a_2, \ldots, a_r) \) of elements of \( GF(q) \) such that \( a_j - a_i \in C(i,j) = C(s_i, s_j) \) for every \( 1 < i < j < r \), or for every \( 1 < s_i < s_j < s_r \).

Hence, in this section, we will deal with a choice function \( C: P(S) \rightarrow \mathcal{C} \) for an \( r \)-set \( S \subseteq N \) instead of a choice function \( C: P(r) \rightarrow \mathcal{C} \).

We are now going to define a choice function \( C_i: P(B_i) \rightarrow \mathcal{C} \) for each \( i \in I_b \) in such a way that they 'will not cross each other' in the sense described below. We will do this by induction on \( i \).

For \( i = 1 \), let \( B_1 = \{ b_{1,1}, b_{1,2}, \ldots, b_{1,k_1} \} \) where \( k_1 = |B_1| \in \mathbb{K} \) and \( 1 \leq b_{1,1} < b_{1,2} < b_{1,3} < \ldots < b_{1,k_1} \leq m \). Define the choice function \( C_1: P(B_1) \rightarrow \mathcal{C} \) in any manner. By Theorem 1.11, there
exists a $k_1$-tuple $T_1 = (a_{1,1}, a_{1,2}, \ldots, a_{1,k_1})$ of elements of $GF(q)$ such that $a_{1,t} - a_{1,s} \in C_1(b_{1,s}, b_{1,t})$ for every $b_{1,s}, b_{1,t} \in B_1$ with $1 \leq b_{1,s} < b_{1,t} \leq m$. Let

$$B_1 = \{(b_{1,1,a_{1,1}}, (b_{1,2,a_{1,2}}, \ldots, (b_{1,k_1,a_{1,k_1}})\}.$$

For $i = 2$, let $B_2 = \{b_{2,1,1}, b_{2,2,1}, \ldots, b_{2,k_2}\}$ where

$$k_2 = |B_2| \in K$$

and $1 \leq b_{2,1} < b_{2,2} < \ldots < b_{2,k_2} \leq m$. For every pair $(b_{2,s}, b_{2,t}) \in P(B_2)$, define $C_2(b_{2,s}, b_{2,t})$ as follows.

If $(b_{2,s}, b_{2,t}) \notin B_1$, then define $C_2(b_{2,s}, b_{2,t})$ to be any element of $\mathcal{H}^e$. However, if $(b_{2,s}, b_{2,t}) \subseteq B_1$, then, since $(I_m, B)$ is an $(m,K,e)$-PBD, we have that $e \geq 2$ and, hence,

$$|\mathcal{H}^e| = e \geq 2.$$ Define $C_2(b_{2,s}, b_{2,t})$ to be any element of $\mathcal{H}^e \setminus \{C_1(b_{2,s}, b_{2,t})\}$. Thus, we have defined a choice function $C_2 : P(B_2) \rightarrow \mathcal{H}^e$ such that $C_2(i,j) \neq C_2(i,j)$ for every $(i,j) \in B_1 \cap B_2$ with $1 \leq i < j \leq m$. By Theorem 1.11, there exists a $k_2$-tuple $T_2 = (a_{2,1}, a_{2,2}, \ldots, a_{2,k_2})$ of elements of $GF(q)$ such that $a_{2,t} - a_{2,s} \in C_2(b_{2,s}, b_{2,t})$ for every $(b_{2,s}, b_{2,t}) \in B_2$ with $1 \leq b_{2,s} < b_{2,t} \leq m$. Let

$$B_2^* = \{(b_{2,1,a_{2,1}}, (b_{2,2,a_{2,2}}), \ldots, (b_{2,k_2,a_{2,k_2}})\}.$$

Assume that we have defined $C_1, C_2, \ldots, C_{r-1}$ for $1 \leq r < b$. Let us now define $C_r$. Let $B_r = \{b_{r,1}, b_{r,2}, \ldots, b_{r,k_r}\}$ where $k_r = |B_r| \in K$ and $1 \leq b_{r,1} < b_{r,2} < \ldots < b_{r,k_r} \leq m$. For every pair $(b_{r,s}, b_{r,t}) \in P(B_r)$, define $C_r(b_{r,s}, b_{r,t})$ as
follows. If \( \{ b_r, s', b_r, t \} \not\subseteq B_1 \cup B_2 \cup \ldots \cup B_{r-1} \), then we define \( C_r(b_r, s', b_r, t) \) to be any element of \( \mathcal{H}^e \). If \( \{ b_r, s', b_r, t \} \subseteq B_1 \cup B_2 \cup \ldots \cup B_{r-1} \), say \( \{ b_r, s', b_r, t \} \subseteq B_i \cap B_{i+1} \cap \ldots \cap B_n \) where \( 1 \leq i_1 < i_2 < \ldots < i_n \leq r-1 \), then we have \( e > n \) and \( |\mathcal{H}^e| = e > n \) since \( (I^*_m, \mathcal{B}) \) is an \((m, K, e) - \text{PBD}\). Define \( C_r(b_r, s', b_r, t) \) to be an element of \( \mathcal{H}^e \backslash \{ C_{i_1}(b_r, s', b_r, t), C_{i_2}(b_r, s', b_r, t), \ldots, C_{i_n}(b_r, s', b_r, t) \} \).

Thus, we have defined a choice function \( C_r : P(B_r) \rightarrow \mathcal{H}^e \) such that \( C_r(i, j) \in \mathcal{H}^e \backslash \{ C_{i_1}(i, j), C_{i_2}(i, j), \ldots, C_{i_n}(i, j) \} \) if \( \{i, j\} \subseteq B_i \cap B_{i+1} \cap \ldots \cap B_n \) where \( 1 \leq i_1 < i_2 < \ldots < i_n \leq r-1 \) (i.e. they do not 'cross each other'). By Theorem 1.11, there exists a \( k_r \)-tuple \( T_r = (a_{r,1}, a_{r,2}, \ldots, a_{r,k_r}) \) of elements of \( \text{GF}(q) \) such that \( a_{r,t} - a_{r,s} \in C_r(b_r, s', b_r, t) \) for every \( \{b_r, s', b_r, t\} \subseteq B_r \) with \( 1 \leq b_r, s < b_r, t \leq m \). Let \( B_r^* = \{(b_r, 1, a_{r,1}), (b_r, s, a_{r,2}), \ldots, (b_r, k_r, a_{r,k_r})\} \).

Hence, we can define \( C_i \), \( i = 1, 2, \ldots, b \), inductively and these \( C_i \)'s do not 'cross each other,' i.e., we have, for every \( 1 \leq i < j \leq m \), that \( \mathcal{H}^e = \{ C_{r_1}(i, j), C_{r_2}(i, j), \ldots, C_{r_e}(i, j) \} \) if \( B_{r_1}, B_{r_2}, \ldots, B_{r_e} \) are the blocks of \( \mathcal{B} \) containing \( \{i, j\} \) (this is true because of the definitions for those choice functions \( C_r \)'s and the fact that \( (I^*_m, \mathcal{B}) \) is an \((m, K, e) - \text{PBD}\)). Further, we have, for each \( r \in I_b \), that if \( B_r = \{b_r, 1, b_r, 2, \ldots, b_r, k_r\} \)
is a block of \((I_m, B)\) where \(k_r = |B_r|\) and
\[1 \leq b_{r,1} < b_{r,2} < \ldots < b_{r,k_r},\]
then we get a
\[B_r^* = \{(b_{r,1}, a_{r,1}), (b_{r,2}, a_{r,2}), \ldots, (b_{r,k_r}, a_{r,k_r})\} \subseteq X\]
such that \(a_{r,t} - a_{r,s} \in C_r(b_{r,s}, b_{r,t})\) for every \([b_{r,s}, b_{r,t}] \subseteq B_r\)
with \(1 \leq b_{r,s} < b_{r,t} \leq m\).

Let \(\{i,j\} \subseteq I_m\) be any 2-set with \(i < j\). Let
\[B_{r_1}, B_{r_2}, \ldots, B_{r_e}\]
be the blocks of \((I_m, B)\) containing \(\{i,j\}\).
Consider the set
\[S_{i,j} = \{a_{r_u,t_u} - a_{r_u,s_u} | b_{r_u,s_u} = i, b_{r_u,t_u} = j,\]
\[1 \leq s_u < t_u < k_{r_u}, 1 \leq u \leq e\}.

By what we just observed, \(S_{i,j}\) forms a system of representatives
for the cosets of \(GF(q)^*\) modulo the e-th powers of \(w\) (i.e., \(H^e\)). Now let \(q - 1 = de\). Let \(T \subseteq GF(q)^*\) be any subset, say
\(T = \{t_1, t_2, \ldots, t_n\}\). We will use \(aT\) to denote the set
\(\{at_1, at_2, \ldots, at_n\}\) for any \(a \in GF(q)^*\). Since \(S_{i,j}\) is a system of representatives for \(H^e\), it is easily seen that
\[w^{xe}S_{i,j} \cap w^{ye}S_{i,j} = \emptyset\] for any 2-set \([x, y] \subseteq \{0, 1, 2, \ldots, d - 1\}\)
\[d - 1\]
and \[\bigcup_{y=0}^{d-1} w^{ye}S_{i,j} = GF(q)^*\]. This is true for any \(\{i,j\} \subseteq I_m\)
with \(i < j\).
Now let $B_{x,y}^* = w^y B_{x}^*$ for $x \in I_b$ and $y \in \{0,1,2,\ldots,d-1\}$. Let $\mathcal{A}^* = \{B_{x,y}^* \mid x \in I_b \text{ and } y = 0, 1, 2, \ldots, d - 1\}$. By what we just observed, we have that $\Delta(\mathcal{A},(i,j)) = GF(q)^*$ for every $1 \leq i < j \leq m$. By Proposition 4.2, we have completed the proof of the following very important theorem.

**Theorem 4.8.** Let $m, e \in \mathbb{N}$ be given positive integers. Let $K \subseteq \mathbb{N}$ be a finite set. Suppose that an $(m,K,e)$-PBD exists. Let $q \in \mathbb{N}$ be a prime power such that $q \equiv 1 \pmod{e}$ and $q > e^{\max(K)(\max(K) - 1)}$. Then there exists an LD$(q,m,K)$.

If $K = \{k\}$, we have, by Corollary 4.7, a corollary of this theorem.

**Corollary 4.9.** Let $m,k \in \mathbb{N}$ be given. Let $e = t \beta_1^*(m,k) \in \mathbb{N}$ for any $t \in \mathbb{N}$ with $t > \tilde{T}(m,k)$ obtained in Corollary 4.7. Let $q$ be a prime power such that $q \equiv 1 \pmod{e}$ and $q > e^{k(k-1)}$. Then an LD$(q,m,k)$ exists.

However, as for $K$, we have another corollary of Theorem 4.8 with the help of Corollary 4.5.

**Corollary 4.10.** Let $K \subseteq \mathbb{N}$ be a given finite set. Let $m \in \mathbb{N}$ be a positive integer such that $m > M_0(K)$ (see Corollary 4.4). Let $e = t \beta_1^*(m,K) \in \mathbb{N}$ for any $t \in \mathbb{N}$. Let $q \in \mathbb{N}$ be a prime power such that $q \equiv 1 \pmod{e}$ and $q > e^{\max(K)(\max(K) - 1)}$. Then an LD$(q,m,K)$ exists.
§4.3 The Statement of the Existence Theorem for $\lambda = 1$.

First of all, let us recall the result proved in [8].

Theorem 4.11. For every $k \in \mathbb{N}$, there exists a constant $c(k)$ such that $m \in OA[k]$ for every positive integer $m > c(k)$.

As remarked in §1.3, $oa(k)$ is the smallest integer for which Theorem 4.11 holds. Let $K \subseteq \mathbb{N}$ be given. Recall the finite set $K_0 \subseteq K$, in §4.1, such that $\beta(K_0) = \beta(K)$, $\alpha(K_0) = \alpha(K)$, $\gamma(K_0) = \gamma(K)$ and $M(K_0) = M_0(K)$ (see Corollary 4.4). Let $A = \text{Max}(oa(k + 1) \mid k \in K_0)$. If $K = \{k\}$, let $M_1(K) = oA(k + 1)$. Otherwise, let $M_1(K) = \text{Max}(A, M_0(K))$. For the rest of this chapter, we will fix this $M_1(K)$. Now we are ready to state the existence theorem for $LD(n, m, K)$.

Theorem 4.12. Let $K \subseteq \mathbb{N}$ be a given subset of positive integers such that $k \geq 3$ for every $k \in K$. Given a positive integer $m > M_1(K)$, there exists a constant $\widetilde{C} = \widetilde{C}(m, K)$ such that $n \in \text{NHG}[m, K]$ for every positive integer $n > \widetilde{C}$ satisfying (4.1) and (4.2).

Let $\widetilde{C}(m, K)$ be the smallest integer for which Theorem 4.12 holds. By Proposition 4.1, (4.1) and (4.2) are equivalent to (4.3) and (4.4). By Corollary 1.35, $\text{NHG}[m, K]$ is a closed set. In order to prove Theorem 4.12, it is sufficient, in view of Theorem 1.10, to show that $\beta(\text{NHG}[m, K]) = \beta^*(m, K)$ and $\alpha(\text{NHG}[m, K]) = \alpha^*(m, K)$.
The next two sections are devoted to computing $\beta(\text{NHG}[m,K])$ and $\alpha(\text{NHG}[m,K])$.

As we remarked in §4.1, we will have a corresponding result for $\text{NVG}[m,K]$ which we will not state. The modifications to the statement and the proof of this theorem are easily seen.

§4.4 The Existence of $\text{LD}(n,m,k)$. In this section, we will compute $\beta(\text{NHG}[m,k])$ and $\alpha(\text{NHG}[m,k])$. Then, we will use this result to prove Theorem 4.12 for $K$ in the next section. First of all, let us remark that the restriction $m > M_1([k])$ is not needed for the computing of $\beta(\text{NHG}[m,k])$ as we shall see in the course of the proof. Now, let us observe an important lemma which is very similar to Lemma 2.17.

**Lemma 4.13.** Let $d, c \in \mathbb{N}$. Assume that $d$ is even. Define the set $Q = \{q \in \mathbb{N} | q$ is a prime power, $q > c$, and $q \equiv 1 \pmod{d}\}$. Then $\beta(Q) = d$.

**Proof:** For any $q \in Q$, $d|q(q - 1)$. Thus, $d|\beta(Q)$, say $\beta(Q) = ds$ for some $s \in \mathbb{N}$. We claim that $s = 1$. Assume not. Let $p$ be a prime divisor of $s$.

By the same argument as in Lemma 2.17, we observe that either $(dp, d(p+1) + 1) = 1$ or $(dp, d(p-1) + 1) = 1$. Without loss of generality, assume that $(dp, d(p+1) + 1) = 1$. By Dirichlet's theorem (Theorem 2.16), there exists a prime number $q = dpt + d(p + 1) + 1 > \max(c, \beta(Q))$ for some $t \in \mathbb{N}$. Thus,
\[ q \equiv 1 \pmod{d} \] and \( q \in \mathbb{Q} \). Therefore, \( \beta(q) | q(q - 1) \). Since
\( q \) is a prime and \( q > \beta(q) \), \( \beta(q) | q - 1 \). Thus \( ds | dpt + d(p + 1) \),
i.e. \( s | pt + p + 1 \). Since \( p \) is a prime divisor of \( s \),
\( p | pt + p + 1 \), a contradiction. Therefore, \( s = 1 \). Hence
\( \beta(q) = d \), as desired.

Now we are ready to prove

**Theorem 4.14.** Let \( k \geq 3 \) be given positive integer. Let
\( m \in \mathbb{N} \) be a given positive integer. Then \( \beta(\text{NHG}[m,k]) = \beta^{\ast}(m,k) \).

**Proof:** By the definitions of \( \beta^{\ast}_{1}(m,k) \) and \( \beta^{\ast}(m,k) \), we see
that \( \beta^{\ast}(m,k) = \epsilon(\beta^{\ast}_{1}(m,k)) \) where \( \epsilon \) is defined in §2.1. In
view of Corollary 4.7, let \( p_{1} \) and \( p_{2} \) be two distinct prime
numbers such that \( p_{1} > \widetilde{T}(m,k) \) and \( p_{2} > \widetilde{T}(m,k) \). Then both
\( (m,k,p_{1}\beta^{\ast}_{1}(m,k)) \)-BIBD and \( (m,k,p_{2}\beta^{\ast}(m,k)) \)-BIBD exist. Let
\( e_{1} = p_{1}\beta^{\ast}_{1}(m,k) \) and \( e_{2} = p_{2}\beta^{\ast}(m,k) \). Define the sets

\[ Q_{1} = \{ q \in \mathbb{N} | q \text{ is a prime power, } q > e_{1}^{k(k-1)}, \text{ and } q \equiv 1 \pmod{e_{1}} \}, \]

\[ Q_{2} = \{ q \in \mathbb{N} | q \text{ is a prime power, } q > e_{2}^{k(k-1)}, \text{ and } q \equiv 1 \pmod{e_{2}} \}. \]

By Corollary 4.9, \( Q_{1} \subseteq \text{NHG}[m,k] \) and \( Q_{2} \subseteq \text{NHG}[m,k] \). Thus,
\( \beta(\text{NHG}[m,k]) | \beta(Q_{1}) \) and \( \beta(\text{NHG}[m,k]) | \beta(Q_{2}) \). By Lemma 4.13, we have
that \( \beta(\text{NHG}[m,k]) | (\beta(Q_{1}),\beta(Q_{2})) = (e_{1},e_{2}) = \beta^{\ast}(m,k) \).
Now, by Proposition 4.1, $\beta^*(m,k)|n(n - 1)$ for all $n \in NHG[m,k]$. Thus, $\beta^*(n,k)|\beta(NHG[m,k])$. Hence, $\beta(NHG[m,k]) = \beta^*(m,k)$.

By Corollary 1.35, NHG[m,k] is a closed set. As a consequence of Theorems 4.14 and 2.19, we have

**Corollary 4.15.** Let $m, k \in \mathbb{N}$ be given as in the theorem. Then there exists a constant $C = C(m,k)$ such that, for any $t \in NHG[m,k]$, we have

$$\{n \in \mathbb{N} | n \geq C, n \equiv t \pmod{\beta^*(m,k)}\} \subseteq NHG[m,k].$$

In particular,

$$\{n \in \mathbb{N} | n \geq C, n \equiv 1 \pmod{\beta^*(m,k)}\} \subseteq NHG[m,k].$$

Since $\beta^*(m,k) | k(k - 1)$, $\{n \in \mathbb{N} | n \geq C, n \equiv 1 \pmod{k(k - 1)}\} \subseteq NHG[m,k]$. Now, let us observe the following simple fact.

**Lemma 4.16.** Let $m, k \in \mathbb{N}$ be given as in Theorem 4.14. Suppose that $\beta^*_1(m,k)$ is even. Then we have $$(\beta(NHG[m,k]), k - 1) = \alpha^*(m,k).$$

**Proof:** By assumption, $\beta^*(m,k) = \beta^*_1(m,k)$. By Theorem 4.14, $\beta(NHG[m,k]) = \beta^*(m,k)$. Now it is easy to see that
\[(\beta(\text{NHG}[m,k]), k - 1) = (\beta^*(m,k), k - 1)\]
\[= (\beta^*_1(m,k), k - 1)\]
\[= \alpha^*(m,k) .\]

**Theorem 4.17.** Let \(k, m \in \mathbb{N}\) be any two positive integers such that \(m \in \text{OA}^T[k]\). Then \(\alpha(\text{NHG}[m,k]) = \alpha^*(m,k)\).

**Proof:** For notational convenience, we shall write, in the course of the proof, \(\alpha\) and \(\beta\) for \(\alpha(\text{NHG}[m,k])\) and \(\beta(\text{NHG}[m,k])\), respectively. By assumption, there is a TPD(\(k, m\)) with one parallel class (transversal design with one parallel class). Let \((X, \mathcal{A}, \mathcal{B}, \mathcal{C})\) be such a TPD\((k, m)\). As remarked in §1.4, \((X, \mathcal{A}, \mathcal{B}, \mathcal{C})\) is an LD\((k, m, k)\). Therefore, \(k \in \text{NHG}[m, k]\). Hence \(\alpha | k - 1\), by the definition of \(\alpha(\text{NHG}[m,k])\). By definition, \(\alpha | \beta\). Therefore, \(\alpha | (\beta, k - 1)\).

By Proposition 4.1, \(\alpha^*(m,k) | n - 1\) for all \(n \in \text{NHG}[m,k]\). Hence \(\alpha^*(m,k) | \alpha\). It remains to show that \(\alpha | \alpha^*(m,k)\). We have two cases.

**Case 1.** \(k\) is even. Since \(k - 1\) is odd,
\[(2\beta^*_1(m,k), k - 1) = (\beta^*_1(m,k), k - 1) .\]

Thus, we conclude that
\[(\beta, k - 1) = (\beta^*_1(m,k), k - 1) = \alpha^*(m,k) .\]

Hence, \(\alpha | (\beta, k - 1) = \alpha^*(m,k)\). Therefore, \(\alpha = \alpha^*(m,k)\).
Case 2. \( k \) is odd. First, let us assume that \( m \) is even. Since \( k - 1 \) is even and \( m - 1 \) is odd, \( (k - 1, m - 1) \) and \( (m(m - 1), k) \) are odd. Thus, \( \beta_1^*(m,k) \) is even. By Lemma 4.16, 
\[ \alpha|\beta(k - 1) = \alpha^*(m,k). \] Hence \( \alpha = \alpha^*(m,k) \). So, let us assume that \( m \) is odd. If \( \beta_1^*(m,k) \) is even, then we have the result by Lemma 4.16. Hence, we may assume that \( \beta_1^*(m,k) \) is odd. Since \( m, k \), and \( \beta_1^*(m,k) \) are odd, \( \frac{k - 1}{(m - 1, k - 1)} \) is odd. Also, \( \beta = 2\beta_1^*(m,k) \) and, hence, \( (\beta, k - 1) = 2 \frac{k - 1}{(m - 1, k - 1)} \). Therefore, we have that \( \alpha^*(m,k) | \alpha \) and \( \alpha | 2\alpha^*(m,k) \). It remains to show that \( \alpha \) is odd.

By Corollary 4.7, let \( t \in \mathbb{N} \) an odd integer such that \( t > \tilde{T}(m,k) \). Then an \( (m,k, t\beta_1^*(m,k)) \)-BIBD exists. Let \( e = t\beta_1^*(m,k) \). Since \( e \) is odd, \( 2 \) is a unit modulo \( e \) (since the reduced residue classes of \( \mathbb{Z}_e \) form a group under multiplication). Then there exists \( a \in \mathbb{N} \) such that \( 2^a \equiv 1 \pmod{e} \). Let \( n \in \mathbb{N} \) be an integer such that \( n \) is an multiple of \( a \) and \( 2^n > e^{k(k - 1)} \). By Corollary 4.9, there exists an \( LD(2^n, m,k) \). Thus, \( 2^n \in \text{NHG}[m,k] \). By the definition of \( \alpha(\text{NHG}[m,k]) \), \( \alpha | 2^n - 1 \) which is odd. Thus, \( \alpha \) is odd and \( \alpha = \alpha^*(m,k) \), as desired.

Now if \( m > M_1([k]) = \Omega(k + 1) \), Theorem 4.11 yields that \( m \in \Omega[k + 1] \). Thus, a \( \text{TD}(k + 1, m) \) exists. By Proposition 1.29, \( m \in \Omega^T[k] \). Therefore, we have
Corollary 4.18. Let \( k \geq 3 \) be a given positive integer.

Let \( m \in \mathbb{N} \) be such that \( m > M_1([k]) \) defined in §4.3. Then 
\[
\alpha(\text{NHG}[m,k]) = \alpha^*(m,k).
\]

By the remark made right after Theorem 4.12, we have proved Theorem 4.12 for \( K = \{k\} \).

§4.5 The Existence of LD(n,m,K).

As we did in §4.4, we shall first compute \( \beta(\text{NHG}[m,K]) \).

Theorem 4.19. Let \( K \subseteq \mathbb{N} \) be a set of positive integers such that \( k \geq 3 \) for every \( k \in K \). Let \( m \in \mathbb{N} \) be such that \( m > M_o(K) \) (see Corollary 4.4). Then \( \beta(\text{NHG}[m,K]) = \beta^*(m,K) \).

Proof: Recall, in §4.1, the finite set \( K_o \subseteq K \) such that 
\[
\beta(K_o) = \beta(K), \quad \gamma(K_o) = \gamma(K), \quad \alpha(K_o) = \alpha(K), \quad \text{and} \quad M_o(K) = M(K_o).
\]

Thus, \( \beta^*(m,K_o) = \beta^*(m,K) \). Let \( k_o = \max(K_o) \). In view of Corollary 4.5, let \( e = \beta^*(m,K_o) \). Then an \( (m,K_o,e) \) - PBD exists. Define the set
\[
Q = \{ q \in \mathbb{N} \mid q \text{ is a prime power, } q > e^{k_o(k_o - 1)}, \quad q \equiv 1 \pmod{e} \}.
\]

By Corollary 4.10, \( Q \subseteq \text{NHG}[m,K_o] \). Thus, \( \beta(\text{NHG}[m,K_o])|\beta(q) = e = \beta^*(m,K_o) \), by Lemma 4.13.

Now, by Proposition 4.1, \( \beta^*(m,K_o)|n(n - 1) \) for every \( n \in \text{NHG}[m,K_o] \). Thus, \( \beta^*(m,K_o)|\beta(\text{NHG}[m,K_o]) \). Hence, 
\[
\beta(\text{NHG}[m,K_o]) = \beta^*(m,K_o). \quad \text{By the choice of } K_o, \quad \beta(\text{NHG}[m,K_o]) = \beta^*(m,K_o) = \beta^*(m,K). \quad \text{Now, since } K_o \subseteq K, \quad \text{NHG}[m,K_o] \subseteq \text{NHG}[m,K].
\]

Therefore, we have that \( \beta(\text{NHG}[m,K])|\beta(\text{NHG}[m,K_o]) = \beta^*(m,K_o) = \)
\( \beta^*(m,K) \). Again by Proposition 4.1, \( \beta^*(m,K) \mid n(n - 1) \) for every \( n \in \text{NHG}[m,K] \). Thus, \( \beta^*(m,K) \mid \beta(\text{NHG}[m,K]) \). Hence, \( \beta(\text{NHG}[m,K]) = \beta^*(m,K) \).

By the definition of \( M_1(K) \), Theorem 4.19 is still valid if we replace the phrase '\( m > M_\circ(K) \)' by '\( m > M_1(K) \)'.' By Corollary 1.35, \( \text{NHG}[m,K] \) is a closed set. Thus, we have, as a very easy consequence of Theorems 4.18 and 2.19, the following.

**Corollary 4.19.** Let \( K \subseteq \mathbb{N} \) and \( m \in \mathbb{N} \) be given as in Theorem 4.18. Then there exists a constant \( C = C(m,K) \) such that, for any \( t \in \text{NHG}[m,K] \), \( \{n \in \mathbb{N} \mid n \geq C, n \equiv t \pmod{\beta^*(m,K)} \} \subseteq \text{NHG}[m,K] \). In particular, \( \{n \in \mathbb{N} \mid n \geq C, n \equiv 1 \pmod{\beta^*(m,K)} \} \subseteq \text{NHG}[m,K] \).

Now, observe the following simple lemma which is similar to Lemma 3.9.

**Lemma 4.20.** Let \( m \in \mathbb{N} \) be a given positive integer \( > 1 \). Let \( K \subseteq \mathbb{N} \) be any set of positive integers \( > 1 \). Let \( S = \left\{ \frac{k - 1}{(m - 1, k - 1)} \mid k \in K \right\} \). Then \( \gcd(S) = \frac{\alpha(K)}{(m - 1, \alpha(K))} \).

**Proof:** The proof is very similar to that of Lemma 3.9.

Let \( K \subseteq \mathbb{N} \) be a set of positive integers such that \( k \geq 3 \) for every \( k \in K \). Recall, in §4.1, the finite set \( K_\circ \subseteq K \) such that \( \beta(K_\circ) = \beta(K) \), \( \alpha(K_\circ) = \alpha(K) \), \( \gamma(K_\circ) = \gamma(K) \),
\( M_0(K) = M(K_0) \). Recall also the number \( M_1(K) = \text{Max}(A, M_0(K)) \)
where \( A = \text{Max}\{Oa(k+1) \mid k \in K_0\} \). Now we are ready to prove

**Theorem 4.22.** Let \( K \subseteq \mathbb{N} \) be a set of positive integers
such that \( k \geq 3 \) for every \( k \in K \). Let \( m \in \mathbb{N} \) be such that
\( m > M_1(K) \). Then \( \alpha(\text{NHG}[m,K]) = \alpha^*(m,K) \).

**Proof:** By the choice of \( K_0 \subseteq K \), we have, in particular,
that \( \alpha(K) = \alpha(K_0) \). Therefore, \( \alpha^*(m,K_0) = \alpha^*(m,K) \). By
Proposition 4.1, \( \alpha^*(m,K) \mid n - 1 \) for every \( n \in \text{NHG}[m,K] \).
Thus, \( \alpha^*(m,K) \mid \alpha(\text{NHG}[m,K]) \). Since \( K_0 \subseteq K \), \( \text{NHG}[m,K_0] \subseteq \text{NHG}[m,K] \).
Thus, \( \alpha(\text{NHG}[m,K]) \mid \alpha(\text{NHG}[m,K_0]) \). Now, for every \( k \in K_0 \),
\( \text{NHG}[m,k] \subseteq \text{NHG}[m,K_0] \). Thus, we have that \( \alpha(\text{NHG}[m,K_0]) \mid \alpha(\text{NHG}[m,k]) \).
By Corollary 4.17, \( \alpha(\text{NHG}[m,k]) = \alpha^*(m,k) = \frac{k - 1}{(m - 1,k - 1)} \).
Therefore, \( \alpha(\text{NHG}[m,K_0]) \mid \frac{k - 1}{(m - 1,k - 1)} \) for every \( k \in K_0 \). By
Lemma 4.20, we have that \( \alpha(\text{NHG}[m,K_0]) \mid \alpha(K_0) \).
Therefore, we have that \( \alpha^*(m,K) \mid \alpha(\text{NHG}[m,K]) \),
\( \alpha(\text{NHG}[m,K]) \mid \alpha(K_0) \), and \( \alpha(\text{NHG}[m,K_0]) \mid \alpha^*(m,K_0) \).
But \( \alpha^*(m,K) = \alpha^*(m,K_0) \). We have that \( \alpha(\text{NHG}[m,K]) = \alpha^*(m,K) \).

By the remark made right after Theorem 4.12, we have completed
the proof of Theorem 4.12.

§4.6 The Existence of \( \text{LD}(n,m,K,\lambda) \). In this section, we
will prove one of our main results, namely,
Theorem 4.23. Let $K \subseteq \mathbb{N}$ be a set of positive integers $\geq 3$. There exists a constant $M_1$, depending on $K$, with the property that if $m > M_1$ is a given positive integer and $\lambda$ is a given positive integer, then there exists a constant $\tilde{C} = \tilde{C}(m,K,\lambda)$ such that an LD$(n,m,K,\lambda)$ exists for every positive integer $n > \tilde{C}$ satisfying (1.9) and (1.10).

Let $\tilde{C}(m,K,\lambda)$ be the smallest integer for which Theorem 4.23 holds. First of all, let us observe

Proposition 4.24. Let $m \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Let $\lambda \in \mathbb{N}$ be a given positive integer such that $\lambda = \sum_{j=1}^{s} a_j \lambda_j$ where $a_j \geq 0, \lambda_j \geq 1, j \in I_s$. Then $\bigcap_{j=1}^{s} \text{NHG}[m,K,\lambda_j] \subseteq \text{NHG}[m,K,\lambda]$.

Proof: Let $n \in \bigcap_{j=1}^{s} \text{NHG}[m,K,\lambda_j]$. Then there exists an LD$(n,m,K,\lambda_j)$, say $(X,\gamma,H,\sigma_j)$, for each $j \in I_s$. Define a family $\mathcal{A} = a_1 \sigma_1 + a_2 \sigma_2 + \ldots + a_s \sigma_s$. Then $(X,\gamma,H,\sigma)$ is an LD$(n,m,K,\lambda)$.

Corollary 4.25. Let $m \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Let $\lambda, \lambda_0 \in \mathbb{N}$ be such that $\lambda_0 | \lambda$. Then $\text{NHG}[m,K,\lambda_0] \subseteq \text{NHG}[m,K,\lambda]$.

Let $m \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given as in Theorem 4.23. Let $\lambda \in \mathbb{N}$. Let $\lambda_0 = (\lambda_0,\beta(K))$. Then $(\lambda_0,\beta(K)) = (\lambda_0,\beta(K))$. Since $\alpha(K) | \beta(K)$, $(\alpha,\alpha(K)) = (\alpha_0,\alpha(K))$. Therefore, (1.9) and (1.10) are
equivalent to \( \lambda_0 (m - 1)n(n - 1) \equiv 0 \pmod{\beta(K)} \) and 
\( \lambda_0 (n - 1)(m - 1) \equiv 0 \pmod{\alpha(K)} \), since \( \lambda \) can be written as 
\( \lambda_0 \cdot b \) where \( b \in \mathbb{N} \) and \( (b, \beta(K)) = (b, \alpha(K)) = 1 \). Given 
m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) as in Theorem 4.23, if Theorem 4.23 is true for 
\( \lambda_0 \), then it is also true for \( \lambda \) since \( \text{NHG}[m, K, \lambda_0] \subseteq \text{NHG}[m, K, \lambda] \). 
Therefore, with given \( m \in \mathbb{N} \) and \( K \subseteq \mathbb{N} \) as in Theorem 4.23, 
Theorem 4.23 is true for all \( \lambda \in \mathbb{N} \) iff it is true for those 
\( \lambda \in \mathbb{N} \) which divides \( \beta(K) \). In particular, if Theorem 4.23 is 
true, the constant \( \tilde{c}(m, K, \lambda) \) can be chosen to be independent of 
\( \lambda \). Thus Theorem 4.23 can be rephrased as

**Theorem 4.23'.** Let \( K \) be a set of positive integers \( \geq 3 \). 
There exists a constant \( M_1 \), depending on \( K \), with the property 
that if \( m > M_1 \) is a given positive integer and \( \lambda \) is a given 
positive integer, then there exists a constant \( \tilde{c} = \tilde{c}(m, K) \) such 
that an \( \text{LD}(n, m, K, \lambda) \) exists for all positive integers \( n > \tilde{c} \) 
satisfying (1.9) and (1.10).

Let us observe

**Proposition 4.26.** Let \( m, \lambda \in \mathbb{N} \) be any two positive integers. 
Let \( K \subseteq \mathbb{N} \) be a set of positive integers. Then (1.9) and (1.10) 
are equivalent to

\[
n(n - 1) \equiv 0 \pmod{\varepsilon\left(\frac{\beta^*(m, K)}{(\lambda, \beta^*(m, K))}\right)}, \quad \text{and} \quad (4.11)
\]
\[ n - 1 \equiv 0 \pmod{\frac{\alpha^*(m,K)}{(\lambda,\alpha^*(m,K))}} \quad (4.12) \]

where \( \epsilon \) is defined as in \$2.1.\)

**Proof:** The proof is very similar to that of Proposition 3.14.

Thus, Theorem 4.23' can be rephrased as

**Theorem 4.23".** Let \( K \subseteq \mathbb{N} \) be a set of positive integers \( \geq 3 \). There exists a constant \( M_1 \), depending on \( K \), such that if \( m > M_1 \) is a given positive integer and \( \lambda \) is a given positive integer, then there exists a constant \( \bar{c} = \bar{c}(m,K) \) such that an \( LD(n,m,K,\lambda) \) exists for all positive integers \( n > \bar{c} \) satisfying (4.11) and (4.12).

Before proving Theorem 4.23", let us note

**Proposition 4.27.** Let \( m \) and \( \lambda \) be two positive integers. Let \( K \subseteq \mathbb{N} \) be given. Suppose that \( \alpha(NHG[m,K]) = \alpha^*(m,K) \) and \( \beta(NHG[m,K]) = \beta^*(m,K) \). Then \( \beta(NHG[m,K,\lambda]) = \beta^*(m,K,\lambda) \) and \( \alpha(NHG[m,K,\lambda]) = \alpha^*(m,K,\lambda) \), where \( \beta^*(m,K,\lambda) = \epsilon \left( \frac{\beta^*(m,K)}{(\lambda,\beta^*(m,K))} \right) \) and

\[ \alpha^*(m,K,\lambda) = \frac{\alpha^*(m,K)}{(\lambda,\alpha^*(m,K))} \]

**Proof:** By Propositions 1.36 and 4.26, \( \beta^*(m,K,\lambda) | n(n - 1) \) for every \( n \in NHG[m,K,\lambda] \). By the definition of \( \beta(NHG[m,K,\lambda]) \), \( \beta^*(m,K,\lambda) | \beta(NHG[m,K,\lambda]) \). By Proposition 1.34,
\[ B(\text{NHG}[m,K] ; \lambda) \subseteq \text{NHG}[m,K,\lambda] \]. Hence, \( \beta(\text{NHG}[m,K,\lambda]) \mid \beta(B(\text{NHG}[m,K] ; \lambda)) \).

By Proposition 3.15 and our assumption that \( \beta(\text{NHG}[m,K]) = \beta^*(m,K) \), we have that \( \beta(B(\text{NHG}[m,K] ; \lambda)) = \beta^*(m,K,\lambda) \) and \( \beta(\text{NHG}[m,K,\lambda]) \mid \beta^*(m,K,\lambda) \). Hence, \( \beta(\text{NHG}[m,K,\lambda]) = \beta^*(m,K,\lambda) \).

By propositions 1.36 and 4.26, \( \alpha^*(m,K,\lambda) \mid n - 1 \) for every \( n \in \text{NHG}[m,K,\lambda] \). By the definition of \( \alpha(\text{NHG}[m,K,\lambda]) \),

\[
\alpha^*(m,K,\lambda) \mid \alpha(\text{NHG}[m,K,\lambda])
\]

By Proposition 1.34,

\[ B(\text{NHG}[m,K] ; \lambda) \subseteq \text{NHG}[m,K,\lambda] \]. Hence \( \alpha(\text{NHG}[m,K,\lambda]) \mid \alpha(B(\text{NHG}[m,K] ; \lambda)) \).

By Proposition 3.15 and the assumption that \( \alpha(\text{NHG}[m,K]) = \alpha^*(m,K) \),

we have that \( \alpha(B(\text{NHG}[m,K] ; \lambda)) = \alpha^*(m,K,\lambda) \) and \( \alpha(\text{NHG}[m,K,\lambda]) \mid \alpha^*(m,K,\lambda) \). Hence \( \alpha(\text{NHG}[m,K,\lambda]) = \alpha^*(m,K,\lambda) \).

**Proof of Theorem 4.23"** Let \( M_1 = M_1(K) \) where \( M_1(K) \) is defined in §4.3. By Corollary 1.35, \( \text{NHG}[m,K,\lambda] \) is a closed set. In order to prove Theorem 4.23", it is sufficient, in view of Theorem 1.10 and Proposition 4.26, to show that \( \beta(\text{NHG}[m,K,\lambda]) = \beta^*(m,K,\lambda) \) and \( \alpha(\text{NHG}[m,K,\lambda]) = \alpha^*(m,K,\lambda) \). However, we have that \( \beta(\text{NHG}[m,K]) = \beta^*(m,K) \) and \( \alpha(\text{NHG}[m,K]) = \alpha^*(m,K) \) by our assumption, and Theorems 4.19 and 4.22. Now Proposition 4.27 yields the result.

**§4.7 Special Cases.** In this section, we shall prove stronger results than Theorem 4.23 for the existence of \( \text{LD}(n,m,k,\lambda) \) when \( k = 3, 4, 5, \) and \( 6 \).
Proposition 4.28. Let $m$ and $k$ be positive integers such that $m \geq k$ and $m \in OA_{T}^{k}$. Let $\lambda \in \mathbb{N}$ be given. Then there exists a constant $\tilde{C} = \tilde{C}(m,k)$ such that $n \in NHG[m,k,\lambda]$ for all positive integers $n > \tilde{C}$ satisfying

\[
\lambda n(n-1)m(m-1) \equiv 0 \pmod{k(k-1)}, \quad \text{and} \quad \lambda(n-1)(m-1) \equiv 0 \pmod{(k-1)}.
\]

Proof: In view of Theorem 1.10 and Proposition 4.26, it is sufficient to show that $\beta(NHG[m,k,\lambda]) = \beta^{*}(m,k,\lambda)$ and $\alpha(NHG[m,k,\lambda]) = \alpha^{*}(m,k,\lambda)$. By Proposition 4.27, it is sufficient to show that $\beta(NHG[m,k]) = \beta^{*}(m,k)$ and $\alpha(NHG[m,k]) = \alpha^{*}(m,k)$.

However, Theorem 4.14 yields that $\beta(NHG[m,k]) = \beta^{*}(m,k)$ and Theorem 4.17 yields that $\alpha^{*}(NHG[m,k]) = \alpha^{*}(m,k)$. Thus, Theorem 4.23 yields the result.

Theorem 4.29. Let $m \geq 3$ and $\lambda$ be given positive integers. Then there exists a constant $\tilde{C}_{3} = \tilde{C}_{3}(m)$ such that an $LD(n,m,3,\lambda)$ exists for all positive integers $n > \tilde{C}_{3}$ satisfying (4.13) and (4.14) with $k = 3$.

Proof: It was shown [5] that $m \in OA[4]$ for all $m \in \mathbb{N}$ except $m = 2, 6$. By Proposition 1.29, $m \in OA_{T}[3]$ for all $m \in \mathbb{N}$ except $m = 2, 6$. However, Hanani [12] showed that a $TD(3,6)$ existed with 4 parallel classes of blocks. Hence, $m \in OA_{T}[3]$ for every positive integer $m \geq 3$. By Proposition 4.28, we
have the result.

For notational convenience, let \( L(m) \) denote the number of mutually orthogonal Latin squares of order \( m \). It is a well-known theorem (see [10]) that the existence of a \( \text{TD}(k,m) \) is equivalent to the existence of \( k - 2 \) mutually orthogonal Latin squares of order \( m \). By Proposition 1.29, we note that the existence of a \( \text{TD}(k+1, m) \) implies the existence of a \( \text{TPD}(k,m) \) (by deleting one group from a \( \text{TD}(k+1, m) \)).

**Theorem 4.30.** Let \( m \geq 4 \) and \( \lambda \) be given positive integers such that \( m \not\in E_4 \) where \( E_4 = \{6,10,14,15,18,22,26,30,34,38,42,46\} \). Then there exists a constant \( \tilde{c}_4 = \tilde{c}_4(m) \) such that an \( \text{LD}(n,m,4,\lambda) \) exists for all positive integers \( n > \tilde{c}_4 \) satisfying (4.13) and (4.14) with \( k = 4 \).

**Proof:** R. M. Wilson has shown [29] that \( L(m) \geq 3 \) for every positive integer \( m > 46 \). Thus, \( m \in \text{OA}[5] \) for every \( m > 46 \). Therefore, \( m \in \text{OA}^T[4] \) for every \( m > 46 \). By Proposition 4.28, Theorem 4.30 is valid for \( m > 46 \). Let us consider the case for \( 4 \leq m \leq 46 \).

Let \( A_4 = \{4,57,8,9,11,13,16,17,19,23,25,27,29,31,32,37,41,43\} \).

For \( m \in A_4 \), \( m \) is a prime power. \( m \in \text{OA}[5] \) by Proposition 1.30. Thus, \( m \in \text{OA}^T[4] \) for \( m \in A_4 \). By Proposition 4.28, Theorem 4.30 is valid for \( m \in A_4 \).

Let \( A_2 = \{20,28,35,36,40,44,45\} \). By Theorem 1.31, \( m \in \text{OA}[5] \)
for $m \in A_2$. Using the same argument as above, Theorem 4.30 is valid for those $m$'s. Now let $A_3 = \{12, 21, 24, 33\}$. Let $m \in A_3$. Then $\beta(NHG[m,4]) = 6 = \beta^*(m,4)$. Now $m \equiv 0 \text{ or } 1 \pmod{4}$.

It has been shown [12] that $m \in B[4;3]$ for $m \equiv 0 \text{ or } 1 \pmod{4}$.

Thus an $(m,4,3)$-BIBD exists. Now, 2 is a unit in $\mathbb{Z}_3$. Let its order be $a$. Choose $b \in \mathbb{N}$ such that $b$ is a multiple of $a$ and $2^b > 3^{12}$. By Theorem 4.8, an LD($q,m,4$) exists where $q = 2^b$. Thus, $\alpha(NHG[m,4]) | q - 1$ and, hence, $\alpha(NHG[m,4])$ is odd. By Proposition 4.1, $\alpha^*(m,4) = 3 | \alpha(NHG[m,4])$ for $m \in A_3$.

Further, $\alpha(NHG[m,4]) | \beta(NHG[m,4]) = 6$. Therefore, $\alpha(NHG[m,4]) = 3 = \alpha^*(m,4)$. By Proposition 4.27, Theorem 4.30 is valid for $m \in A_3$.

Let us note a theorem in [29] which says that if $0 \leq u \leq t$, then $L(st + u) \geq \min\{L(s), L(s + 1), L(t) - 1, L(u)\}$. Now let $u = 7$, $t = 8$, $s = 4$. Then $L(39) \geq \min\{L(4), L(5), L(8) - 1, L(7)\} = 3$. Thus, a TD$(5,39)$ exists. Hence $39 \in OA^T[4]$. By Proposition 4.28, this theorem is valid for $m = 39$.

**Theorem 4.31.** Let $m \geq 5$ and $\lambda$ be given positive integers such that $m \not\in E_5$ where $E_5 = \{12, 14, 18, 21, 22, 24, 28, 33, 34, 38, 39, 42, 44, 48, 52, 54, 57, 58\}$. Then there exists a constant $\tilde{c}_5 = \tilde{c}_5(m)$ such that an LD$(n,m,5,\lambda)$ exists for all positive integers $n > \tilde{c}_5$ satisfying (4.13) and (4.14) with $k = 5$.

**Proof:** R. M. Wilson has shown [29] that $L(m) \geq 4$ for every $m > 60$. Therefore, $m \in OA^T[5]$ for every $m > 60$. By Proposition
4.28, Theorem 4.31 is valid for \( m > 60 \).

Let \( A_1 = \{5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 31, 32, 37, 41, 43, 47, 49, 53, 59\} \). For \( m \in A_1 \), \( m \) is a prime power and hence \( m \in OA^T[5] \) by Proposition 1.30. Hence, the theorem is valid for \( m \in A_1 \).

Let \( A_2 = \{35, 40, 45, 55, 56\} \). For \( m \in A_2 \), \( m \in OA^T[5] \) by Theorem 1.31. Hence the theorem is valid for \( m \in A_2 \).

Let \( A_3 = \{6, 10, 20, 26, 30, 36, 46, 50, 60\} \). Let \( m \in A_3 \).

Then \( \beta(NHG[m,5]) = \beta^*(m,5) = 4 \). Thus, \( \alpha(NHG[m,5])|\beta(NHG[m,5]) = 4 \).

By Proposition 4.1, \( \alpha^*(m,5) = 4|\alpha(NHG[m,5]) \). Hence \( \alpha(NHG[m,5]) = 4 \). By Proposition 4.27, Theorem 4.31 is valid for \( m \in A_3 \).

Let \( A_4 = \{15, 51\} \). For \( m \in A_4 \), \( \beta(NHG[m,5]) = \beta^*(m,5) = 2 \).

Thus, \( \alpha(NHG[m,5])|\beta(NHG[m,5]) = 2 \). By Proposition 4.1, \( \alpha^*(m,5) = 2|\alpha(NHG[m,5]) \). Hence, \( \alpha(NHG[m,5]) = \alpha^*(m,5) = 2 \).

By Proposition 4.27, Theorem 4.31 is valid for \( m \in A_4 \).

This completes the proof of this theorem.

**Theorem 4.32.** Let \( m \geq 6 \) and \( \lambda \) be given positive integers such that \( m \notin E_6 \) where \( E_6 = \{14, 20, 26, 35, 38, 44, 50, 62\} \).

Then there exists a constant \( \tilde{C}_6 = \tilde{C}_6(m) \) such that an \( \text{LD}(n,m,6,\lambda) \) exists for all positive integers \( n > \tilde{C}_6 \) satisfying (4.13) and (4.14) with \( k = 6 \).
Proof: It has been shown [14] that \( L(m) \geq 5 \) for every \( m > 62 \). Therefore, \( m \in OA^T[6] \) for every \( m > 62 \).

By Proposition 4.28, this theorem is valid for \( m > 62 \).

Let us consider the cases when \( 6 \leq m \leq 62 \).

Let \( A_1 = \{7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59, 61\} \). For \( m \in A_1 \), \( m \) is a prime power and hence \( m \in OA^T[6] \) by Proposition 1.30. Hence the theorem is valid for \( m \in A_1 \).

For \( m = 56 \), \( m \in OA^T[6] \) by Theorem 1.31. Hence the assertion is valid for \( m = 56 \).

Let \( A_2 = \{10, 12, 15, 18, 22, 24, 28, 30, 33, 34, 39, 40, 42, 45, 48, 52, 54, 55, 57, 58, 60\} \). Let \( m \in A_2 \). Then
\[ \beta(NHG[m, 6]) = \beta^*(m, 6) = 10. \]
Thus, \( \alpha(NHG[m, 6]) \mid 10 \).

Now \( m \equiv 0 \) or \( 1 \) (mod 3). It has been shown [16] that an \((m, 6, 5)\)-BIBD exists for \( m \equiv 0 \) or \( 1 \) (mod 3).

Now 2 is a unit in \( \mathbb{Z}_5 \). Let \( a \) be its order in \( \mathbb{Z}_5 \).

Let \( b \in \mathbb{N} \) be a multiple of \( a \) such that \( 2^b > 5^{30} \).

By Theorem 4.8, there exists an \( LI(2^b, m, 6) \). Then
\[ \alpha(NHG[m, 6]) \mid 2^b - 1 \] which is odd. By Proposition 4.1,
\[ \alpha^*(m, 6) = 5 \mid \alpha(NHG[m, 6]) \] Hence \( \alpha(NHG[m, 6]) = \alpha^*(m, 6) = 5 \).

By Proposition 4.28, the theorem is valid for \( m \in A_2 \).

Let \( A_3 = \{6, 21, 36, 46, 51\} \). Let \( m \in A_3 \). Then
\[ \beta(NHG[m, 6]) = \beta^*(m, 6) = 2. \] Hence \( \alpha(NHG[m, 6]) \mid \beta(NHG[m, 6]) = 2 \).
However, \( m = 0 \) or 1 (mod 3). By the same argument as above, we get that \( \alpha \) is odd. Hence \( \alpha(NHG[m, 6]) = 1 = \alpha^*(m, 6) \).

By Proposition 4.28, the theorem is valid for \( m \in A_3 \).
§5.1 Preliminaries. Let $s \in \mathbb{N}$ and $R \subseteq \mathbb{Z}$ be given. A residue class $r \in \mathbb{Z}_s$ is called a fiber mod $s$ of $R$ iff there is some $n \in R$ such that $n \equiv r \pmod{s}$. Let $K \subseteq \mathbb{Z}$ be a given set. Let $F$ be the image set of $K$ under the canonical epimorphism $\mathbb{Z} \to \mathbb{Z}_p(K)$. Then, for every $k \in K$, there is some $f \in F$ such that $k \equiv f \pmod{p(K)}$. Now, one of the main results in [26, 27] is

Theorem 5.1. Let $K$ be a closed set. There is a constant $M$ such that, for every $f \in F$,

$$\{n \in \mathbb{N} \mid n \geq M, n \equiv f \pmod{p(K)}\} \subseteq K.$$ 

Given two sets $S, T \subseteq \mathbb{N}$, we say that $S$ and $T$ eventually coincide iff there is a constant $C$ such that

$$\{s \in S \mid s \geq C\} = \{t \in T \mid t \geq C\}.$$ 

Thus, Theorem 5.1 means that
\{k \in K \mid k \geq M \} = \bigcup_{f \in F} \{n \in \mathbb{N} \mid n \geq M, n \equiv f \ (\text{mod} \ \beta(K))\},

where \( F \), as before, is the image of \( K \) under the canonical epimorphism \( \mathbb{Z} \to \mathbb{Z}_{\beta(K)} \).

§5.2 Sub-GDD's. Let \( K \subseteq \mathbb{N} \) be a given subset. Let \( n_0, m_0, n \) and \( m \) be given positive integers such that \( n \geq n_0 \) and \( m \geq m_0 \).

**Definition.** Let \((X, \mathcal{A}, \mathcal{D})\) be a GD\((n, m, K)\) where \( \mathcal{A} = \{G_i \mid i \in I_n\} \).

Let \((X', \mathcal{A}', \mathcal{D}')\) be a GD\((n_0, m_0, K)\) where \( \mathcal{A}' = \{G'_j \mid j \in I_{n_0}\} \). We say that \((X', \mathcal{A}', \mathcal{D}')\) is a sub-GDD of \((X, \mathcal{A}, \mathcal{D})\) if

(i) \( X' \subseteq X \),

(ii) \( \mathcal{A}' \subseteq \mathcal{A} \),

(iii) for each \( j \in I_{n_0} \), there is a unique \( i_j \in I_n \) such that \( G'_j \subseteq G_i \) and \( i_{j_1} \neq i_{j_2} \) for any \( j_1 \neq j_2 \in I_{n_0} \).

Now suppose that a GD\((n_0, m_0, K)\) exists. Define the set

\[ S_K(n_0, m_0, m) = \{n \in \mathbb{N} \mid \text{there is a GD}(n, m, K) containing a GD}(n_0, m_0, K) \text{ as a sub-GDD}\}. \]
Lemma 5.2. \( S_K(n_0, m_0, m) \cup \{1\} \) is a closed set.

Proof: It suffices to show that \( B[S_K(n_0, m_0, m) \cup \{1\}] \subseteq S_K(n_0, m_0, m) \cup \{1\} \). Let \( n \in B[S_K(n_0, m_0, m) \cup \{1\}] \). We may assume that \( n > 1 \). Thus, there is an \( (n, S_K(n_0, m_0, m) \cup \{1\}, 1) \)-PBD, say \((X, \mathcal{A})\).

Let \( w: X \to \mathbb{N} \) be a weighting such that \( w(x) = m \) for every \( x \in X \). For each \( B \in \mathcal{A} \) with \( |B| \neq 1 \), \( |B| \in S_K(n_0, m_0, m) \).

Hence, there is a GD(|B|, m, K) containing a GD(n_0, m_0, K) as a sub-GDD. In fact, we need only one such GDD and use the regular GD(|B|, m, K) for the remaining blocks \( B \) of \( \mathcal{A} \). By the construction of Theorem 1.18, there is a GD(n, m, K) containing a GD(n_0, m_0, K) as a sub-GDD, i.e. \( n \in S_K(n_0, m_0, m) \cup \{1\} \).

Lemma 5.3. Let \( K \subseteq \mathbb{N} \) be given. Let \( n_0, m_0, t, m \) and \( m \) be given positive integers such that \( n \geq n_0 \), \( t \geq n_0 \), and \( m \geq m_0 \).

Suppose \( n \in NG[mt, K] \) and \( t \in S_K(n_0, m_0, m) \). Then \( nt \in S_K(n_0, m_0, m) \).

Proof: Let \((X, \mathcal{A}, \mathcal{A})\) be a GD(n, mt, K) where \( \mathcal{A} = \{G_i | i \in I_n\} \).

For each \( i \in I_n \), \( |G_i| = mt \in S_K(n_0, m_0, m) \) and, hence, a GD(t, m, K) exists on \( G_i \), say \((G_i, \mathcal{A}_i, \mathcal{A}_i)\) where \( \mathcal{A}_i = \{G_{ij} | j \in I_t\} \).

By hypothesis, let \((Y, \mathcal{N}, \mathcal{A})\) be a GD(n_0, m_0, K) contained in, say \((G_n, \mathcal{A}_n, \mathcal{A}_n)\) as a sub-GDD, where \( \mathcal{N} = \{H_1, H_2, \ldots, H_{n_0}\} \). Then \( Y \subseteq G_n \), \( \mathcal{A} \subseteq \mathcal{A}_n \), and, for each \( u \in I_{n_0} \), there is a unique \( j_u \in I_t \) such that \( j_1 \neq j_2 \) for \( u_1 \neq u_2 \in I_{n_0} \) and \( H_u \subseteq G_{n_0} j_u \).
Now let $\mathcal{J}^* = \{G_{ij} \mid i \in I_n, j \in I_t\}$ and $\mathcal{A}^* = \mathcal{A}_1 + \mathcal{A}_2 + \ldots + \mathcal{A}_n + \mathcal{A}$. Then, by the construction of Lemma 1.17, $(X, \mathcal{J}^*, \mathcal{A}^*)$ is a GD$(nt, m, K)$ containing $(Y, \mathcal{A}, \mathcal{B})$ as a sub-GDD. Hence $nt \in S_K(n_o, m_o, m)$.

**Lemma 5.4.** Let $K \subseteq \mathbb{N}$ be given. Let $n_o, m_o, t, n$, and $m$ be given positive integers such that $n \geq n_o$ and $m \geq m_o$. Suppose $n \in S_K(n_o, m_o, mt)$ and $t \in NG[m, K]$. Then $nt \in S_K(n_o, m_o, m)$.

**Proof:** Let $(X, \mathcal{J}, \mathcal{A})$ be a GD$(n, mt, K)$ containing a GD$(n_o, m_o, K)$, say $(Y, \mathcal{A}, \mathcal{B})$, as a sub-GDD where $\mathcal{J} = \{G_i \mid i \in I_n\}$ and $\mathcal{A} = \{H_i \mid i \in I_{n_o}\}$. Then $Y \subseteq X$, $\mathcal{B} \subseteq \mathcal{A}$, and, for each $u \in I_{n_o}$, there is a unique $i_u \in I_n$ such that $i_u \neq i_{u'}$ for $u \neq u' \in I_{n_o}$ and $H_u \subseteq G_{i_u}$. For notational convenience, we may assume that $i_u = u$ for every $u \in I_{n_o}$, i.e. $H_u \subseteq G_u$ for every $u \in I_{n_o}$.

By hypothesis, there is a GD$(t, m, K)$, say $(G_i, \mathcal{J}_i, \mathcal{A}_i)$, on $G_i$ for every $i \in I_n$ where $\mathcal{J}_i = \{G_{ij} \mid j \in I_t\}$. Since $|G_{ij}| = m$, $|H_u| = m_o$, and $m \geq m_o$, we may assume, for notational convenience, that $H_u \subseteq G_{u,1}$ for every $u \in I_{n_o}$.

Now let $\mathcal{J}^* = \{G_{ij} \mid i \in I_n, j \in I_t\}$ and $\mathcal{A}^* = \mathcal{A}_1 + \mathcal{A}_2 + \ldots + \mathcal{A}_n + \mathcal{A}$. By the construction of Lemma 1.17, $(X, \mathcal{J}^*, \mathcal{A}^*)$ is a GD$(nt, m, K)$ containing $(Y, \mathcal{A}, \mathcal{B})$ as a sub-GDD, i.e. $nt \in S_K(n_o, m_o, m)$.

This lemma states, actually, that 'breaking up groups'
preserves sub-GDD. Now we are ready to prove the following important theorem on sub-GDD's.

Theorem 5.5. If, for some \( n \in N \), there is a GD\((n,m,K)\) containing a GD\((n_0,m_0,K)\) as a sub-GDD, then NG\([m,K]\) and \(S_K(n_0,m_0,m)\) eventually coincide.

Proof: If \( \beta(NG[m,K]) = 0 \), then NG\([m,K]\) = \([1]\) and the assertion is obvious. So, we assume that \( \beta(NG[m,K]) > 0 \). By hypothesis, \( n \in SK(n_0,m_0,m) \). Hence \( n \geq n_0 \) and \( \beta(S_K(n_0,m_0,m)) \mid n(n-1) \). Therefore \( \beta(S_K(n_0,m_0,m)) > 0 \).

Let \( u \in Z \beta(S_K(n_0,m_0,m)) \) be a fiber mod \( \beta(S_K(n_0,m_0,m)) \) of NG\([m,K]\). Let \( r \in NG[m,K] \) with \( r \equiv u(\text{mod} \ \beta(S_K(n_0,m_0,m))) \). Then there is a GD\((r,m,K)\), say \((X,\mathcal{J},\mathcal{A})\). Let \( T = \{|B| \mid B \in \mathcal{A} \} \). Then \( T \) is a finite set. By Lemma 5.2, \( S_K(n_0,m_0,m) \cup \{1\} \) is a closed set. Now \( 1 \text{mod} \ \beta(S_K(n_0,m_0,m)) \) is a fiber of the closed set \( S_K(n_0,m_0,m) \cup \{1\} \). By Theorem 5.1, there are infinitely many \( t \in S_K(n_0,m_0,m) \) with \( t \equiv 1 \text{mod} \ \beta(S_K(n_0,m_0,m)) \). Choose such a \( t \) that \( t > \text{Max} \ \text{oa}(c) \) where \( \text{oa}(c) \) is as defined in §1.3. Then a GD\((c,t,c)\) exists for every \( c \in T \). Let \( w: X \to N \) be a weighting defined by \( w(x) = t \) for every \( x \in X \). By Theorem 1.18, a GD\((r,mt,K)\) exists. But, by the choice of \( t \), we obtain that \( rt \in S_K(n_0,m_0,K) \) with the help of Lemma 5.3. But \( rt \equiv u(\text{mod} \ \beta(S_K(n_0,m_0,m))) \). Hence \( u \) is also a fiber mod \( \beta(S_K(n_0,m_0,m)) \) of \( S_K(n_0,m_0,m) \cup \{1\} \).
Conversely, every fiber mod $\beta(S_K(n_o,m_o,m))$ of $S_K(n_o,m_o,m) \cup \{1\}$ is also a fiber mod $\beta(S_K(n_o,m_o,m))$ of $NG[m,K]$, since $S_K(n_o,m_o,m) \cup \{1\} \subseteq NG[m,K]$. Therefore, $S_K(n_o,m_o,m) \cup \{1\}$ and $NG[m,K]$ have the same fibers mod $\beta(S_K(n_o,m_o,m))$.

For every $x \in NG[m,K]$, there is some $f \in \mathbb{Z}_{\beta(S_K(n_o,m_o,m))}$ such that $x \equiv f \pmod{\beta(S_K(n_o,m_o,m))}$. But since $S_K(n_o,m_o,m) \cup \{1\}$ and $NG[m,K]$ have the same fibers mod $\beta(S_K(n_o,m_o,m))$, there is $y \in S_K(n_o,m_o,m)$ such that $y \equiv f \pmod{\beta(S_K(n_o,m_o,m))}$. Thus, $x \equiv y \pmod{\beta(S_K(n_o,m_o,m))}$.

Now since $\beta(S_K(n_o,m_o,m)) | \gamma(y - 1)$, we obtain that $\beta(S_K(n_o,m_o,m)) | x(x - 1)$ for every $x \in NG[m,K]$. Therefore, $\beta(S_K(n_o,m_o,m)) | \beta(NG[m,K])$. But since $S_K(n_o,m_o,m) \subseteq NG[m,K]$, we have that $\beta(NG[m,K]) | \beta(S_K(n_o,m_o,m))$. Hence $\beta(NG[m,K]) = \beta(S_K(n_o,m_o,m))$. Thus, $NG[m,K]$ and $S_K(n_o,m_o,m) \cup \{1\}$ have the same fibers mod $\beta(S_K(n_o,m_o,m)) = \beta(NG[m,K])$. By Theorem 5.1, they eventually coincide.

This theorem says that if there is, for some $n_1 \in \mathbb{N}$, a GD($n_1$,m,K) containing a GD($n_o$,m_o,K), say $(X,\mathcal{A},\gamma)$, as a sub-GDD (i.e. $S_K(n_o,m_o,m) \neq \emptyset$), then there exists a GD(n,m,K) containing $(X,\mathcal{A},\gamma)$ as a sub-GDD for all 'sufficiently large' $n \in NG[m,K]$.

Corollary 5.6. NG[m_o,K] and $S_K(n_o,m_o,m)$ eventually coincide.
Proof: Clear, since \( n_0 \in NG[\,m_0, K] \cap S_K(n_0, m_0, m) \).

As before, let \( m_0, n_0 \in \mathbb{N} \) be given positive integers such that a GD\((n_0, m_0, K)\) exists. The next theorem gives a sufficient condition under which there is, for some \( n_0 \in \mathbb{N} \), a GD\((n_1, m, K)\) containing a GD\((n_0, m_0, K)\) as a sub-GDD.

Theorem 5.7. Let \( m, m_0 \) be given positive integers such that \( m \geq m_0 \). Let \( K \) be a set of positive integers. Let \( n_0 \) be a positive integer such that a GD\((n_0, m_0, K)\) exists. If

\[
\frac{m_0}{(m, m_0)} \cdot \alpha(K) = 1
\]

then \( NG[m, K] \) and \( S_K(n_0, m_0, m) \) eventually coincide.

Proof: In view of Theorem 5.5, it suffices to exhibit, for some \( n \in \mathbb{N} \), a GD\((n, m, K)\) containing a GD\((n_0, m_0, K)\) as a sub-GDD. By hypothesis, there are \( a, b \in \mathbb{Z} \) such that

\[
a \cdot \frac{m_0}{(m, m_0)} + b \cdot \alpha(K) = 1.
\]

Now, since \((a + s \alpha(K)) \cdot \frac{m_0}{(m, m_0)} + (b - s \cdot \frac{m_0}{(m, m_0)}) \cdot \alpha(K) = 1\) for any \( s \in \mathbb{N} \), we may assume that \( a \in \mathbb{N} \). Hence,

\[
a \cdot \frac{m_0}{(m, m_0)} \equiv 1 \pmod{\alpha(K)} \tag{5.1}
\]

By Lemma 2.1, there are \( c, d \in \mathbb{Z} \) such that

\[
c \cdot \gamma(K) + d \cdot \alpha(K) = 1.
\]
Now, \((c + t \alpha(k))\gamma(k) + (d - t \gamma(k))\alpha(k) = 1\) for any \(t \in \mathbb{N}\).

So, we may assume that \(c \in \mathbb{N}\). Thus, we have

\[ c \gamma(k) \equiv 1 \pmod{\alpha(k)} \quad (5.2) \]

Combining (5.1) and (5.2), we obtain that

\[ ac \gamma(k) \equiv 1 \pmod{\alpha(k)} \]

Recall the fact that \(\beta(k) = \alpha(k)\gamma(k)\). Therefore, \(ac \gamma(k)\frac{m}{(m, m_0)} \equiv 1 \pmod{\alpha(k)}\) is a positive solution in \(n\) for the system of congruence equations

\[ n(n - 1)m^2 \equiv 0 \pmod{\beta(k)}, \quad \text{and} \quad (5.3) \]

\[ (n - 1)m \equiv 0 \pmod{\alpha(k)}. \quad (5.4) \]

By Theorem 2.4, there exists a constant \(N_o = N(m, K)\) such that, if \(n > N_o\) and satisfies (5.3) and (5.4), then \(n \in NG[m, K]\).

Replacing \(a\) by \(a + s \alpha(k)\) and \(c\) by \(c + t \alpha(k)\) for \(s, t \in \mathbb{N}\), we may choose \(s\) and \(t \in \mathbb{N}\) such that

\[(a + s \alpha(k))(c + t \alpha(k))\gamma(k)\frac{m}{(m, m_0)} > N_o.\]

For convenience, let

\[ b = (a + s \alpha(k))(c + t \alpha(k))\gamma(k)\frac{m}{(m, m_0)}. \]

Then

\[ b \equiv 1 \pmod{\alpha(k)} \]

and \(b \in NG[m, K]\) is a solution in \(n\) of (5.3) and (5.4). Thus \(b \in NG[m, K]\).
Again, by Theorem 2.4, $\text{NG}[\frac{m}{(m_o,m)}b, n_o]$ contains all 'sufficiently large' $n \in \mathbb{N}$ which satisfies

$$n(n-1)[\frac{m}{(m_o,m)}b]^2 \equiv 0 \pmod{n_o(n_o-1)},$$

and

$$(n-1)[\frac{m}{(m_o,m)}b] \equiv 0 \pmod{(n_o-1)}.$$

Choose such an $n$ and fix it for the rest of the proof.

Let $(X, \mathcal{A}, \mathcal{D})$ be a GD($n, \frac{m}{(m_o,m)}b, n_o$). Let $w : X \to \mathbb{N}$ be a weighting defined by $w(x) = m_o$ for every $x \in X$. Let $Y_x, x \in X$, be a set of $m_o$ points such that $Y_x \cap Y_y = \emptyset$ for $x \neq y \in X$. Let $X^* = \bigcup_{x \in X} Y_x$, $G^* = \bigcup_{x \in X} Y_x$ for $G \in \mathcal{A}$, and $\mathcal{D}^* = \{G^* | G \in \mathcal{D}\}$. Now we know that a GD($n_0, m_o, K$) exists. For each $B \in \mathcal{A}$, $|B| = n_o$. Suppose $\bigcup_{x \in B} (Y_x | x \in B), \mathcal{D}_B$ is such a GD($n_0, m_o, K$). Let $\mathcal{D}^* = \bigcup_{B \in \mathcal{D}} \mathcal{D}_B$. By the construction of Theorem 1.18, $(X^*, \mathcal{D}^*)$ is a GD($b, \frac{m}{(m,m_o)} m, K$) containing a GD($n_0, m_o, K$) as a sub-GDD.

Now, by the choice of $b$, $b, \frac{m}{(m,m_o)} \in \text{NG}[m,K]$. By Lemma 5.4, we obtain that $nb, \frac{m}{(m,m_o)} \in \text{NG}[m,K]$. Thus, we have a GD($n_1, m, K$) containing a GD($n_0, m_o, K$) as a sub-GDD where $n_1 = nb, \frac{m}{(m,m_o)}$, as desired.
Corollary 5.8. For any $t \in \mathbb{N}$, $NG[tm_0, K]$ and $S_K(n_0, m_0, tm_0)$ eventually coincide.

Proof: Note that $\frac{m_0}{(tm_0, m_0)} = 1$. By Theorem 5.7, we obtain the result.

§5.3 Nonisomorphic GDD's. Let $m, n, \lambda \in \mathbb{N}$ and $K \subseteq \mathbb{N}$ be given. Let $(X_1, \mathcal{B}_1, \mathcal{G}_1)$ and $(X_2, \mathcal{B}_2, \mathcal{G}_2)$ be two given $GD(n, m; K, \lambda)$'s. They are said to be isomorphic iff there exists a bijection $\varphi: X_1 \rightarrow X_2$ such that

(i) $\varphi$ induces an one-to-one correspondence between $\mathcal{B}_1$ and $\mathcal{B}_2$,

(ii) for every $B \subseteq X_1$, $B$ is a block of $\mathcal{G}_1$ iff $\varphi(B)$ is a block of $\mathcal{G}_2$.

We will use $N(n, m, K, \lambda)$ to denote the number of nonisomorphic $GD(n, m, K, \lambda)$'s. From now on, $K = \{k\}$ will be assumed and we shall write $N(n, m, k, \lambda)$ instead of $N(n, m, \{k\}, \lambda)$. In this section, we will show that $N(n, m, k, \lambda) \rightarrow \infty$ as $n \rightarrow \infty$ in a sequence such that the quadruple $(n, m, k, \lambda)$ satisfies the necessary conditions for given $m, k, \lambda \in \mathbb{N}$.

For the rest of this section, let $m, k, \lambda$ be given positive integers. Now, let $n \in \mathbb{N}$ be given and $X$ a given set of $mn$ points. Let $\mathcal{B} = \{G_1, G_2, \ldots, G_n\}$ be a parallel class on $X$ where $|G_i| = m$ for every $i \in \mathbb{I}_n$. Consider the pair
transversal k-family of \((X, \mathcal{A})\) is defined to be a family \(\{Y_i \mid i \in I\}\) of k-subsets of \(X\) such that \(|Y_i \cap G_j| \leq 1\) for every \(i \in I\) and \(j \in I_n\).

**Proposition 5.9.** There exists a constant \(N_o = N_o(m,k,\lambda)\) such that if \(n \in NG[m,k,\lambda]\) and \(n > N_o\), then, for a given pair \((X, \mathcal{B})\) defined as above, there are at least two distinct transversal k-families \(\mathcal{A}\) for which \((X, \mathcal{B}, \mathcal{A})\) is a GD\((n,m,k,\lambda)\).

**Proof:** Let \(N_1 = N_1(m,k,\lambda)\) be such that if \(n > N_1\), then

\[\binom{n}{k} m^k > b = \frac{\lambda n(n - 1)m^2}{k(k - 1)}\]

(the number of blocks in a GD\((n,m,k,\lambda)\)).

Let \(N_2 = N(m,k,\lambda)\) be the number obtained in Theorem 3.11'.

Now let \(N_o = \max(N_2, N_1)\). Let \(n \in NG[m,k,\lambda]\) and \(n > N_o\). Let \((X, \mathcal{B}, \mathcal{A})\) be such a GD\((n,m,k,\lambda)\). Since \(n > N_1\), there exists a k-subset \(Y\) of \(X\) such that \(|Y \cap G| \leq 1\) for every group \(G\) of \(\mathcal{B}\) and \(Y\) is not a block in \(\mathcal{A}\). But, by an appropriate permutation of \(X\) (exchange groups if necessary), we can then find an isomorphic but distinct transversal k-family \(\mathcal{A}'\) such that \((X, \mathcal{B}, \mathcal{A}')\) is a GD\((n,m,k,\lambda)\) in which \(Y\) is a block.

Let \(N_o(m,k,\lambda)\) be the smallest integer for which Proposition 5.9 holds. Let \(r \in \mathbb{W}\) be a given positive integer. Consider the set \(S = \{1\} \cup \{n \in \mathbb{N} \mid n > r\}\). Let \(n \in B[S]\). Let \((X, \mathcal{A})\) be an \((n,S,1)\)-PBD. Hence, \(r < |B| \leq n\) for every block \(B\) of \(\mathcal{A}\). But then \(n \in S\), i.e. \(S = B[S]\). Therefore, \(S\) is a closed
set. The intersection of closed sets is closed. By Corollary 1.21, the set

\[ L = N_0[m, k, \lambda] \cap \{(1) \cup \{n \in \mathbb{N} \mid n > N_0(m, k, \lambda)\}\} \]

is closed.

We now state without proof one of the theorems in [26, 27].

**Theorem 5.10.** If \( K \subseteq \mathbb{N} \) is closed, then there is a finite subset \( K_0 \) of \( K \) such that \( K = B[K_0] \).

Thus, there is a finite set \( K_0 \subseteq L \) such that \( L = B[K_0] \) where \( L \) is defined previously. Now we are ready to prove one of our main results.

**Theorem 5.11.** Let \( m \geq 2, k \geq 3 \), and \( \lambda \) be given positive integers. Then there exist constants \( s = s(m, k, \lambda) > 1 \) and \( \tilde{N} = \tilde{N}(m, k, \lambda) \) such that

\[ N(n, m, k, \lambda) > s^{n^2} \]

for all positive integers \( n > \tilde{N} \) for which a GD\((n, m, k, \lambda)\) exists. In particular, \( N(n, m, k, \lambda) \) tends to infinity as \( n \) increases (with given \( m, k, \) and \( \lambda \)) in a sequence such that the quadruple \((n, m, k, \lambda)\) satisfies the necessary conditions.

**Proof:** Let \( L \) be as in the previous paragraph and \( K_0 \) be a finite subset of \( L \) such that \( L = B[K_0] \). Let \( n \in L = B[K_0] \).
Then there is an \((n,K_0,l)\)-PBD, say \((X,\mathcal{A})\) where \(\mathcal{A}\) may be regarded as a class of subsets of \(X\). Consider the associated \(\text{GD}(n,l,K_0, (X,\tilde{X},\mathcal{A}), \text{as defined in } \S 1.3, \text{where } \tilde{X} = \{\{x\} | x \in X\}.\)

Let \(w: X \to \mathbb{N}\) be a weighting defined by \(w(x) = m\) for every \(x \in X\). Let \(A_x\), for every \(x \in X\), be a set of \(m\) points such that \(A_x \cap A_y = \emptyset\) for \(x \neq y \in X\). Let \(X^* = \bigcup_{x \in X} A_x\) and \(A^*_x = \{A_x | x \in X\}\). Also, for every block \(B \in \mathcal{A}\), let \(B^* = \bigcup_{x \in B} A_x\) and \(A^*_B = \{A_x | x \in B\}\).

Now, for every \(B \in \mathcal{A}\), \(|B| \leq K_0 \leq \text{NG}[m,k,\lambda]\). By Proposition 4.9, there are at least two distinct transversal \(k\)-families \(\mathcal{J}_B\) for which \((B^*, \mathcal{J}_B^*, \mathcal{J}_B)\) is a \(\text{GD}(|B|,m,k,\lambda)\) for every \(B \in \mathcal{A}\). For any such a choice of \(\mathcal{J}_B\), \(B \in \mathcal{A}\), let \(\mathcal{A}^* = \sum B \mathcal{J}_B\), i.e. let \(\mathcal{A}^*\) be the family of blocks by combining all the blocks of those chosen \(\mathcal{J}_B\)'s, \(B \in \mathcal{A}\). By Theorem 1.18, \((X^*, \mathcal{A}^*, \mathcal{B}^*)\) is a \(\text{GD}(n,m,k,\lambda)\). Thus, we have at least \(2^b\) distinct transversal \(k\)-families \(\mathcal{A}^*\) for which \((X^*, \mathcal{A}^*, \mathcal{B}^*)\) is a \(\text{GD}(n,m,k,\lambda)\) where \(b\) is the number of blocks in \(\mathcal{A}\), i.e. \(b = |\mathcal{A}|\).

Given an \(mn\)-set \(Y\) and a parallel class on it, say \(Y = \{H_i | i \in I_n\}\) where \(|H_i| = m\) for \(i \in I_n\). On the set \(Y\) where \(Y\) is regarded as the set of groups, a \(\text{GDD}\) can be isomorphic to at most \((mn)!\) \(\text{GDD}'s\) on the same pair \((Y,\mathcal{N})\) with the same set of parameters. Therefore,
Let $k_0$ be the largest integer in $K_\nu$. Since $(X, B)$ is an $(n, K_\nu, 1)$-PBD, every pair of points of $X$ is contained in exactly one block of $B$. Thus,

the number of pairs of points of

\[ X = \binom{n}{2} = \sum_{B \in B} \left( \frac{|B|}{2} \right). \]  

Since $|B| \in K_\nu$ for every $B \in B$, (5.6) implies that

\[ \binom{n}{2} \leq \binom{k_0}{2} b. \]

Thus,

\[ b \geq \frac{n(n-1)}{k_0(k_0-1)} \]

and, hence, (5.5) implies that

\[ N(n,m,k,\lambda) \geq \frac{n(n-1)}{k_0(k_0-1)} - mn \log_2(mn) \]

Now $n^2$ is the dominant term of the right-hand side of (5.7). Let $\delta \geq 2$ be a real number and let $s = \frac{1}{k_0(k_0-1)}$. Then $s > 1$.

It is readily seen that there is an $n_0 \in \mathbb{N}$ such that for
Let \( n > n_0 \)

\[
\frac{n(n-1)}{k_0(k_0-1)} - mn \log_2(mn) > s_n^2.
\]

Thus, if we put \( \tilde{N} = \max(n_0, N_0(m,k,\lambda)) \) where \( N_0 \) is the number in Proposition 5.9, then

\[
N(n,m,k,\lambda) > s_n^2,
\]

for all \( n > \tilde{N} \) with \( n \in NG[m,k,\lambda] \), as desired.

It is known [27] that there exist constants \( c = c(k,\lambda) > 1 \) and \( v_o = v_o(k,\lambda) \) such that the number of nonisomorphic \((v,k,\lambda)\)-BIBD is \( > c v^2 \) for all \( v > v_o \) for which (1.3) and (1.4) hold. Now a \((v,k,\lambda)\)-BIBD \((X,\mathcal{A})\) can be regarded as a GD\((v,1,k,\lambda)\), \((X,\widetilde{\mathcal{A}})\) where \( \widetilde{X} = \{(x) \mid x \in X\} \). Thus the restriction '\( m \geq 2 \)' in Theorem 5.11 can be replaced by '\( m \in \mathbb{N} \)'. From now on, when we refer to Theorem 5.11, we shall mean \( m \in \mathbb{N} \) instead of \( m \geq 2 \). Let \( \tilde{N}(m,k,\lambda) \) be the smallest integer for which Theorem 5.11 is true.

§5.4 Nonisomorphic LD's. Let \( n,m,\lambda \in \mathbb{N} \) and \( K \leq \mathbb{N} \) be given. Let \( (X_1,\mathcal{V}_1,\mathcal{H}_1,\mathcal{A}_1) \) and \( (X_2,\mathcal{V}_2,\mathcal{H}_2,\mathcal{A}_2) \) be two given LD\((n,m,K,\lambda)\)'s. They are said to be isomorphic iff there exists a permutation \( \phi : X_1 \to X_2 \) such that
(i) \( \varphi \) induces an one-to-one correspondence between
\( V_1 \) and \( V_2 \),

(ii) \( \varphi \) induces an one-to-one correspondence between
\( \mathcal{N}_1 \) and \( \mathcal{N}_2 \),

(iii) for every \( B \subseteq X_1 \), \( B \) is a block of \( \mathcal{A}_1 \) iff
\( \varphi(B) \) is a block of \( \mathcal{A}_2 \).

We will use \( N_L(n,m,K,\lambda) \) to denote the number of nonisomorphic
LD\((n,m,K,\lambda)\)'s. From now on, \( K = \{k\} \) will be assumed and we
shall write \( N_L(n,m,k,\lambda) \) instead of \( N_L(n,m,\{k\},\lambda) \). In this
section, we shall show \( N_L(n,m,k,\lambda) \to \infty \) as \( n \to \infty \) with given
\( m,k,\lambda \in \mathbb{N} \) in a sequence such that the quadruple \((n,m,k,\lambda)\)
satisfies the necessary conditions for the existence of an
LD\((n,m,k,\lambda)\).

Let \( n,m,k, \) and \( \lambda \) be given positive integers. Let \( X \)
be a set of \( mn \) points. Let \( V = \{V_1, V_2, \ldots, V_m\} \) be a
parallel class on \( X \) where \( |V_s| = n \) for \( s \in I_m \) and
\( H = \{H_1, H_2, \ldots, H_n\} \) be a parallel class on \( X \) where
\( |H_t| = m \) for \( t \in I_n \). Suppose that \( |V_s \cap H_t| = 1 \) for every
\( s \in I_m, t \in I_n \). Consider the triple \((X,V,H)\). A lattice
k-family of \((X,V,H)\) is defined to be a family \((Y_i | i \in I)\),
for some indexing set \( I \), of \( k \)-subsets of \( X \) such that
\( |Y_i \cap H_t| \leq 1 \) and \( |Y_i \cap V_s| \leq 1 \) for every \( s \in I_m, t \in I_n, \)
i \in I.
Recall the number $oa(k + l)$, the smallest integer such that if $m > oa(k + l)$, then a $TD(k + l, m)$ exists. For the rest of this section, assume that $m > oa(k + l)$.

Proposition 5.12. Let $k, m$, and $\lambda$ be given positive integers such that $m > oa(k + l)$. Then there exists a constant $L_0 = L_0(m, k, \lambda)$ such that if $n \in NHG[m, k, \lambda]$ and $n > L_0$, then, for a given triple $(X, \gamma, \mathcal{H})$ defined as above, there are at least two distinct lattice $k$-families $\mathcal{A}$ for which $(X, \gamma, \mathcal{H}, \mathcal{A})$ is an $LD(n, m, k, \lambda)$.

Proof: Let $L_1 = L_1(m, k, \lambda)$ be such that if $n > L_1$, then
\[
\binom{n}{k} \cdot \frac{m(m - 1)}{k(k - 1)} = \frac{\lambda n(n - 1)m(m - 1)}{k(k - 1)} \quad \text{(the number of blocks in an LD(n, m, k, \lambda))}.
\]
Let $L_2 = C(m, k, \lambda)$ be the number in Theorem 4.23. Now let $L_0 = \max(L_1, L_2)$.

Let $n \in NHG[m, k, \lambda]$ and $n > L_0$. Let $(X, \gamma, \mathcal{H}, \mathcal{A})$ be such an $LD(n, m, k, \lambda)$. Since $n > L_1$, there exists a $k$-subset $Y$ of $X$ such that $|Y \cap H| \leq 1$ and $|Y \cap V| \leq 1$ for every $H \in \mathcal{H}$ and $V \in \mathcal{H}$, and $Y$ is not a block in $\mathcal{A}$. But, by an appropriate permutation of $X$ (exchange vertical or horizontal groups if necessary), we can find an isomorphic but distinct lattice $k$-family $\mathcal{A}'$ such that $(X, \gamma, \mathcal{H}, \mathcal{A}')$ is an $LD(n, m, k, \lambda)$ in which $Y$ is a block.

Let $L_0(m, k, \lambda)$ be the smallest integer for which Proposition
5.12 holds. Define the set $S = \text{NHG}[m,k,\lambda] \cap \{(l) \cup \{n \in \mathbb{N} \mid n > L(m,k,\lambda)\}$. By the observation made right after Proposition 5.9 and the fact that $\text{NHG}[m,k,\lambda]$ is a closed set (Corollary 1.35), $S$ is a closed set. Now we are ready to prove one of our main results.

Theorem 5.13. Let $k \geq 3$ and $\lambda$ be given positive integers. Let $m > \alpha(k+1)$ be a given positive integer. Then there exist constants $t = t(m,k,\lambda) > 1$ and $\widetilde{L} = \widetilde{L}(m,k,\lambda)$ such that

$$N_L(n,m,k,\lambda) > t^n$$

for all positive integers $n$ for which an $LD(n,m,k,\lambda)$ exists. In particular, $N_L(n,m,k,\lambda)$ tends to infinity as $n$ increases (with fixed $m$, $k$, and $\lambda$) in a sequence such that the quadruple $(n,m,k,\lambda)$ satisfies the necessary conditions.

Proof: By Theorem 5.10, there is a finite set $K_o \subseteq S$ such that $S = E[K_o]$. Let $n \in S$. Then there is an $(n,K_o,1)$-PBD, say $(X,\mathfrak{a})$ where $\mathfrak{a}$ may be regarded as a class of subsets of $X$.

Let $X^* = I_m \times X$, $V_i = \{i\} \times X$ for $i \in I_m$, $H_x = I_m \times \{x\}$ for $x \in X$, $\mathcal{V}^* = \{V_i \mid i \in I_m\}$, and $\mathcal{H}^* = \{H_x \mid x \in X\}$. For every block $B$ of $\mathfrak{a}$, we have $|B| \in K_o \subseteq S \subseteq \text{NHG}[m,k,\lambda]$. By Proposition 5.12, there are at least two distinct lattice $k$-families $\mathfrak{J}_B$'s for which $(I_m \times B, \mathcal{V}_B, \mathcal{H}_B, \mathfrak{J}_B)$ is an
LD(|B|,m,k,\lambda) where \mathcal{V}_B = \{i \times B \mid i \in I_m\} and
\mathcal{H}_B = \{I_m \times \{x\} \mid x \in B\}. For any such choice of \mathcal{J}_B for
B \in \mathcal{B}, let \mathcal{G}^* = \Sigma \mathcal{J}_B. By the proof of Proposition 1.34,
(\mathcal{X}^*,\mathcal{Y}^*,\mathcal{H}^*,\mathcal{G}^*) is an LD(n,m,k,\lambda). Thus, we have at least \(2^b\)
distinct lattice \(k\)-families \(\mathcal{G}^*\) for which \((\mathcal{X}^*,\mathcal{Y}^*,\mathcal{H}^*,\mathcal{G}^*)\) is
an LD(n,m,k,\lambda) where \(b\) is the number of blocks in \(\mathcal{G}\), i.e.
\(b = |\mathcal{G}|\).

By a similar argument as in the proof of Theorem 5.11, we
have
\[
N_L(n,m,k,\lambda) \geq \frac{2^b}{(mn)^{\frac{1}{2}}} \geq 2^{b - mn \log_2(mn)}
\]  

(5.8)

Further, if \(k_0\) is the largest integer in \(K_0\), there exist
constants \(t = t(m,k,\lambda) > 1\) and \(k_o = k_o(m,k,\lambda)\) such that
\[
N_L(n,m,k,\lambda) \geq 2^{\frac{n(n - 1)}{k_0(k_o - 1)}} - mn \log_2(mn)
\]  

\(> t^{\frac{n^2}{2}}\)

Thus, if we put \(\tilde{L} = \max(k_o,L_o(m,k,\lambda))\) where \(L_o(m,k,\lambda)\) is the
number obtained in Proposition 5.12, then
\[
N_L(n,m,k,\lambda) > t^n^2
\]

for all \(n > \tilde{L}\) with \(n \in \text{NHG}[m,k,\lambda]\), as desired.

§5.5 Nonisomorphic TD(k,m)'s. For the rest of this chapter,
the index of pairwise balance will be 1, i.e. \( \lambda = 1 \). First of all, recall that \( \text{TD}(k,m) \) is an \( \text{GD}(k,m,k) \), \( \text{TPD}(k,m) \) is an \( \text{TD}(k,m) \) with one parallel class, and \( \text{OA}^T_{\text{r}}[k] = \{ m \in \mathbb{N} \mid \text{a TPD}(k,m) \text{ exists} \} \). We now state without proof a very useful fact (for proof, see [26]).

**Proposition 5.14.** \( \text{OA}^T_{\text{r}}[k] \) is a closed set with respect to the closure operation \( B \).

It is readily seen that there is only one \( \text{TPD}(3,3) \) on a given 9-set \( X \) with groups \( \{G_1,G_2,G_3\} \) where \( |G_i| = 3 \), \( i = 1, 2, 3 \), and \( X = \bigcup_{i=1}^{3} G_i \). However, we have the following fact.

**Proposition 5.15.** Let \( k \geq 3 \) be a given positive integer. For every \( m \in \text{OA}^T_{\text{r}}[k] \) with \( m > 3 \), there exist at least two distinct \( \text{TPD}(k,m) \)'s, \((X,\mathcal{P},\mathcal{A})\) and \((X,\mathcal{P},\mathcal{A}')\) with \( |X| = km \), \( \mathcal{A} = \{G_i \mid i \in I_k\} \), \( \mathcal{P} = \{H_j \mid j \in I_m\}, |G_i| = m \) for \( i \in I_k \), \( |H_j| = k \) and \( j \in I_m \), and \( \mathcal{A} \neq \mathcal{A}' \).

**Proof:** Let \( m \in \text{OA}^T_{\text{r}}[k] \) and \( m > 3 \). Consider \( X = I_m \times I_k \), \( G_i = I_m \times \{i\} \) for every \( i \in I_k \), \( C_j = \{j\} \times I_k \) for every \( j \in I_m \), \( \mathcal{A} = \{G_i \mid i \in I_k\} \), and \( \mathcal{P} = \{C_j \mid j \in I_m\} \). Let \((X,\mathcal{P},\mathcal{A},\mathcal{A}')\) be a \( \text{TPD}(k,m) \). Consider the elements \( C_1 \) and \( C_2 \) of \( \mathcal{P} \). First, assume that \( k = 3 \). Thus \( C_1 = \{(1,1),(1,2),(1,3)\} \) and \( C_2 = \{(2,1),(2,2),(2,3)\} \). Let \( B \) be a block of \( \mathcal{A} \).
containing \((1,1)\). Then either \(B = C_1\) or \(B \cap C_2 \subseteq \{(2,2), (2,3)\}\). But the number of blocks of \(\mathcal{C}\) containing \((1,1)\) is \(m \geq 4\). Hence there is at least one block \(B\) containing \((1,1)\) and two other points from \(X - (C_1 \cup C_2)\), say \(B = ((1,1), (a,2), (b,3))\) where \(a, b \in I_m\). Since \(C_a, C_b \in \mathcal{P}\) are blocks in the \(\text{TD}(k, m)\), \((X, \& \cup \mathcal{P})\), \(a \neq b\). Consider the permutation \(\varphi\) on \(X\) which interchanges \((1,1)\) and \((2,1)\), \((1,2)\) and \((2,2)\), and \((1,3)\) and \((2,3)\), and leaves everything else fixed. Then the image of \(B\) under \(\varphi\) is \(B' = ((2,1), (a,2), (b,3))\) which is not a block of \(\mathcal{C}\) since \(((a,2), (b,3)) \notin B' \cap B\). Let the image of \(\mathcal{C}\) under the 'induced' permutation of \(\varphi\) on \(\mathcal{C}\) be \(\mathcal{C}'\).

Then \((X, \mathcal{P}, \& \cup \mathcal{C})\) and \((X, \mathcal{P}, \& \cup \mathcal{C}')\) are two distinct \(\text{TPD}(k, m)\)'s.

Now assume that \(k > 3\), i.e. \(k \geq 4\). We will use the same notations as above. For simplicity, consider the two points \((1,1)\) and \((2,2)\). They are contained in a unique block \(B\) of \(\mathcal{C}\). Since \(|B| = k \geq 4\), it contains another two points, say \((a, i)\) and \((b, j)\) where \(a, b \in I_m\) and \(i, j \in I_k\). Surely, \(i \neq j\). Since \(C_a, C_b \in \mathcal{P}\) are blocks in the \(\text{TD}(k, m)\), \((X, \& \cup \mathcal{P})\), \(a \neq b\). Consider the permutation \(\varphi\) on \(X\) which interchanges \((1, s)\) and \((2, s)\) for every \(s \in I_k\) and leaves everything else fixed. Then the image \(B'\) of \(B\) under \(\varphi\) will contain \((2,1), (1,2), (a, i)\) and \((b, j)\). Thus \(B'\) is not a block of \(\mathcal{C}\) since \(((a, i), (b, j)) \notin B' \cap B\). Hence, as before, there are at least two distinct \(\text{TPD}(k, m)\)'s.
Let \( \text{NGD}(n,m,k,\lambda) \) denote the number of distinct \( \text{GD}(n,m,k,\lambda) \)'s on a given \( nm \)-set with a given set of groups.

**Corollary 5.16.** Let \( k \geq 3 \) and \( m \) be given positive integers. Let \( J \subseteq \mathbb{N} \) be a given subset. Suppose that there is a \( \text{GDD} \), \((X,\mathcal{A},\lambda)\), with \( |X| = m \), block size \( k \), and group sizes from \( J \). Let \( n \in \text{OA}^T[k] \) with \( n > 3 \) be given. Suppose that a \( \text{GD}(n,|G|,k) \) exists for every \( G \in \mathcal{A} \). Then \( n \in \text{NG}[m,k] \) and, in particular, \( \text{NGD}(n,m,k,1) \geq 2^b \) where \( b \) is the number of blocks in the \( \text{GDD} \), \((X,\mathcal{A},\lambda)\).

**Proof:** For every block \( B \) of \( \mathcal{A} \), \( |B| = k \). Consider \( B \times I_n \) and \( B_b = \{b\} \times I_n \) for every \( b \in B \). Let \( \mathcal{B}_B = \{B_b \mid b \in B\} \). Let \( B_i = B \times \{i\} \) for \( i \in I_n \) and \( \mathcal{B}_B = \{B_i \mid i \in I_n\} \). Since \( n \in \text{OA}^T[k] \) and \( n > 3 \), there are at least two distinct \( \text{TPD}(k,n) \)'s, by Proposition 5.15. Let \((B \times I_n, \mathcal{B}_B, \mathcal{A}_B)\) be one of these \( \text{TPD}(k,m) \)'s. Then \((B \times I_n, \mathcal{B}_B, \mathcal{A}_B)\) is an \( \text{LD}(k,n,k) \). As observed in §1.4, there is an \( \text{LD}(n,k,k) \), namely, \((B \times I_n, \mathcal{B}_B, \mathcal{A}_B, \mathcal{A}_B)\) (exchanging the roles of vertical and horizontal groups). Thus, an \( \text{LD}(n,k,k) \) exists for every block of the \( \text{GDD} \), \((X,\mathcal{A},\lambda)\). By Proposition 1.33, \( n \in \text{NG}[m,k] \), i.e. a \( \text{GD}(n,m,k) \) exists.

For each of these distinct \( \text{TPD}(k,n) \)'s on \( B \times I_n \) for \( B \in \mathcal{A} \), we have a distinct \( \text{GD}(n,m,k) \) on \( X \times I_n \) with the groups \( X \times \{i\} \) for \( i \in I_n \). Therefore, \( \text{NGD}(n,m,k,1) \geq 2^b \) where \( b \) is the number of blocks in the \( \text{GDD} \), \((X,\mathcal{A},\lambda)\).
By the remark made right after Proposition 4.9, the set
\((1) \cup \{m \in N \mid m > 3\}\) is a closed set. Since the intersection
of closed sets is a closed set \(OA^T[k] \cap ((1) \cup \{m \in N \mid m > 3\}) =
OA^T[k] \setminus \{3\}\) is a closed set. Let \(OA^T_1[k] = OA^T[k] \setminus \{3\}\). Then
Proposition 4.15 implies that, given \(k \geq 3\), there are at least
two distinct TPD(k,m)'s on a given km-set with \(k\) groups of
size \(m\) for every \(m \in OA^T_1[k]\).

Let \(k \geq 3\) and \(m\) be given positive integers. Let
\((X_1, P_1, \mathcal{A}_1, \mathcal{B}_1)\) and \((X_2, P_2, \mathcal{A}_2, \mathcal{B}_2)\) be two TPD(k,m)'s. They are
said to be isomorphic iff there is a bijection \(\varphi: X_1 \to X_2\) such that

(i) \(\varphi\) induces an one-to-one correspondence between
\(\mathcal{A}_1\) and \(\mathcal{A}_2\),

(ii) \(\varphi\) induces an one-to-one correspondence between
\(\mathcal{P}_1\) and \(\mathcal{P}_2\),

(iii) for every \(B \subseteq X_1\), \(B\) is a block in \(\mathcal{A}_1\) iff \(\varphi(B)\)
is a block in \(\mathcal{A}_2\).

Let \(NT(m,k)\) be the number of nonisomorphic TPD(k,m)'s.

**Theorem 5.17.** Let \(k \geq 3\) be a given positive integer. Then
there exist constants \(u = u(k) > 1\) and \(m_o = m_o(k)\) such that

\[ NT(m,k) > u^m \]  \hspace{1cm} (5.9)

for all \(m > m_o\). In particular,
\[ N(k,m,k,l) > u^m \]

for all \( m > m_o \).

**Proof:** As observed in §1.4, a TPD\((k,m)\) is an LD\((k,m,k,l)\) and vice versa. Further, an LD\((k,m,k,l)\) exists iff an LD\((m,k,k,l)\) exists (exchanging the roles of vertical and horizontal groups). By Theorem 5.13, there exist constants \( u = u(k) > 1 \) and \( m_1 = m_1(k) \) such that

\[ NT(m,k) = N_L(m,k,k,l) > u^m \]

for all \( m > m_1 \) for which \( m \in OA^T[k] \).

As mentioned in §1.3, \( oa(k) \) is the smallest integer such that \( m \in OA[k] \) for all positive integers \( m > oa(k) \). Let \( m_o = \max(m_1,3,oa(k),oa(k+1)) \). By Proposition 1.29, we have

\[
\{ m \in \mathbb{N} \mid m > m_o \} = \{ m \in OA[k+1] \mid m > m_o \} \\
= \{ m \in OA^T[k] \mid m > m_o \} \\
= \{ m \in OA[k] \mid m > m_o \} . \tag{5.10}
\]

Thus, (5.9) is valid for all \( m > m_o \). Furthermore, a TPD\((k,m)\) is a special case of TD\((k,m)\). (5.10) implies that

\[ N(k,m,k,l) > NT(m,k) > u^m \]

for all \( m > m_o \).
Let \( m_0(k) \) be the smallest integer for which Theorem 5.17 holds.

\[ \S 5.6 \quad k = 3 \]. In this section, we will get a lower bound for \( N(n,m,3,1) \).

In the proof of Theorem 4.29, we observed that
\( OA^T[3] = \{m \in \mathbb{N} \mid m \geq 3\} \cup \{1\} \). By Proposition 5.15, there are at least two distinct TPD(3,m)'s on a given 3m-set for every integer \( m \geq 4 \).

If \( n = 3 \), then a GD(n,m,3) is a TD(3,m). In \( \S 5.5 \), we got a lower bound on \( N(3,m,3,1) \). So, we may assume from now on that \( n \geq 4 \) is a given integer. Thus, \( n \in OA^T[3] \).

Recall that, for \( k = 3 \), the necessary conditions (2.1) and (2.2) for the existence of a GD(n,m,3) become

\[ n(n - 1)m^2 \equiv 0 \pmod{6}, \text{ and} \]  \hspace{1cm} (5.11)

\[ (n - 1)m \equiv 0 \pmod{2}. \]  \hspace{1cm} (5.12)

We have several lemmas

**Lemma 5.18.** If \( n \equiv 0 \) or \( 4 \pmod{6} \), then

\[ \frac{m^2 - 2m - 8}{6} \]

\( NGD(n,m,3,1) \geq 2 \)

for all \( m \in \mathbb{N} \) for which (5.11) and (5.12) hold.
Proof: If \( n \equiv 0 \text{ or } 4 \pmod{6} \), then it is easily seen from (5.11) and (5.12) that \( m \equiv 0 \pmod{2} \). By assumption \( n \geq 4 \). We have two cases. Let \( a = \frac{m^2 - 2m - 8}{6} \).

Case 1. \( m \equiv 0 \text{ or } 2 \pmod{6} \). By Proposition 3.20, \( n \in \text{NG}[2,3] \) since \( m \equiv 0 \text{ or } 2 \pmod{6} \). Thus, \( \text{NGD}(n,2,3,1) \geq 1 \geq 2^a \) for \( m = 2 \). Hence we may assume that \( m \geq 6 \). Now \( m+1 \equiv 1 \text{ or } 3 \pmod{6} \) and there is an \((m+1,3,1)\)-BIBD, say \((X,\mathcal{A})\). Let \( x_0 \in X \) be any fixed element. Let \( \mathcal{A}_0 = \{ B \mid B \in \mathcal{A}, x_0 \in B \} \) and \( \mathcal{A}_0' = \{ B \setminus \{x_0\} \mid B \in \mathcal{A}_0 \} \). As in §1.3, delete this point \( x_0 \) from \( X \). Then \( (X \setminus \{x_0\},\mathcal{A}_0',\mathcal{A} \setminus \mathcal{A}_0) \) is a GD\(\frac{m}{2},2,3\). By Proposition 3.20, \( n \in \text{NG}[2,3] \) since \( n \equiv 0 \text{ or } 4 \pmod{6} \). By Corollary 5.16, \( n \in \text{NG}[m,3] \) and \( \text{NGD}(n,m,3,1) \geq 2^b \) where \( b \) is the number of blocks in the GDD \((X \setminus \{x_0\},\mathcal{A}_0',\mathcal{A} \setminus \mathcal{A}_0)\). It is easily seen that \( b = \frac{m^2 - 2m - 8}{6} \). Thus \( \text{NGD}(n,m,3,1) \geq 2^b \geq 2^a \).

Case 2. \( m \equiv 4 \pmod{6} \). By Proposition 3.20, \( n \in \text{NG}[4,3] \) since \( n \equiv 0 \text{ or } 4 \pmod{6} \). Hence \( \text{NGD}(n,4,3,1) \geq 1 \geq 2^a \) for \( m = 4 \). Hence we may assume that \( m \geq 10 \). Now \( m+1 \equiv 5 \pmod{6} \). It is known [33] that, for any odd integer \( m > 1 \), there is an \((m,3,5,1)\)-PBD which has only one block of size 5. Let \((X,\mathcal{A})\) be such a PBD. Let \( B_0 \in \mathcal{A} \) be the unique block of size 5. Let \( x_0 \in B_0 \) be any fixed point. As in Case 1, delete \( x_0 \) from \( X \). Then we obtain a GDD on \( m \) points with block size 3 and group sizes from \{2,4\} (in fact, one group of size 4.
and \( \frac{m - 4}{2} \) groups of size 2). Since \( n \equiv 0 \) or \( 4 \pmod{6} \), \( n \equiv 0 \) or \( 1 \pmod{3} \). By Proposition 3.20, \( n \in \text{NG}[2,3] \) and \( n \in \text{NG}[4,3] \). By Corollary 5.16, \( n \in \text{NG}[m,3] \) and \( \text{NGD}(n,m,3,1) \geq 2^b \) where \( b \) is the number of blocks in the GDD derived from \((X,\mathcal{A})\) by deleting \( x_0 \). In fact, \( b = b' - r_0 \) where \( b' \) is the number of blocks in the PBD \((X,\mathcal{A})\) and \( r_0 \) is the number of blocks of \( \mathcal{A} \) containing \( x_0 \). It is easy to see that \( r_0 = \frac{m - 4}{2} + 1 \) and that

\[
\text{the number of pairs of points of } X = \binom{m+1}{2} = \sum_{B \in \mathcal{A}} \binom{|B|}{2} = \binom{5}{2} + (b' - 1) \binom{3}{2}.
\]

Thus, \( b' = \frac{m^2 + m - 4}{6} \) and \( b = \frac{m^2 - 2m - 8}{6} = a \). Therefore, \( \text{NGD}(n,m,3,1) \geq 2^a \).

**Lemma 5.19.** If \( n \equiv 1 \) or \( 3 \pmod{6} \), then

\[
\text{NGD}(n,m,3,1) \geq 2 \frac{m^2 - 2m - 20}{6}
\]

for all \( m \in \mathbb{N} \) for which (5.11) and (5.12) hold.

**Proof:** If \( n \equiv 1 \) or \( 3 \pmod{6} \), (5.11) and (5.12) are valid for all \( m \in \mathbb{N} \). Recall that \( n \geq 4 \). Let \( a = \frac{m^2 - 2m - 20}{6} \).

**Case 1.** \( m \) is even. In the proof of Lemma 5.18, we only
use the fact that $n \equiv 0$ or $4 \pmod{6}$ implies that $n \equiv 0$ or $1 \pmod{3}$. Now since $n \equiv 1$ or $3 \pmod{6}$, $n \equiv 0$ or $1 \pmod{3}$.

Using the same argument as in the proof of Lemma 5.18, we get that $NGD(n, m, 3, l) \geq 2^a$ since $\frac{m^2 - 2m - 8}{6} > \frac{m^2 - 2m - 20}{6} = a$.

Case 2. $m$ is odd. Let us first assume that $m \equiv 1$ or $3 \pmod{6}$. For $m = 1$, there is an $(n, 3, 1)$-BIBD since $n \equiv 1$ or $3 \pmod{6}$. As in §1.3, a BIBD can be regarded as a GDD with group size 1. Hence a GD(n, 1, 3) exists. Thus $NGD(n, 1, 3, 1) \geq 1 \geq 2^a$ for $m = 1$. Hence we may assume that $m \geq 3$. Now since $m \equiv 1$ or $3 \pmod{6}$, there is an $(m, 3, 1)$-BIBD, say $(X, \mathcal{D})$. Then we have a GD(m, 1, 3), namely $(X, \tilde{X}, \mathcal{D})$ where $\tilde{X} = \{x \mid x \in X\}$. Since $n \equiv 1$ or $3 \pmod{6}$, an $(n, 3, 1)$-BIBD exists and hence a GD(n, 1, 3) exists. Since $n \geq 4$, we have, by Corollary 5.16, that $n \in NG[m, 3]$ and $NGD(n, m, 3, 1) \geq 2^b$ where $b$ is the number of blocks in $\mathcal{D}$. It is easily seen that $b = \frac{m^2 - m}{6}$. Thus, $NGD(n, m, 3, 1) \geq 2^b \geq 2^a$ for $m = 1$ or $3 \pmod{6}$.

Now assume that $m \equiv 5 \pmod{6}$. For $m = 5$, $n \in NG[5, 3]$ by Proposition 3.21. Thus, $N(n, 5, 3, 1) \geq 1 \geq 2^a$ for $m = 5$. Hence we may assume that $m \geq 11$. It is known [34] that, for any odd integer $m > 1$, there is an $(m, \{3, 5\}, 1)$-PBD which has only one block of size 5. Let $(X, \mathcal{D})$ be such a PBD.

Let $B_o \in \mathcal{D}$ be the unique block of size 5. Consider $X^* = X \times I_n$, $G_i = X \times \{i\}$ for $i \in I_n$ and $E^* = \{G_i \mid i \in I_n\}$.

First of all, consider $B_o \times I_n$. By Proposition 3.21, a
GD(n,5,3) exists, say, \((B_o \times I_n, \{B_o \times \{i\} \mid i \in I_n\}, \sigma_o)\).

For each block \(B \in \mathcal{A}\) of size 3, consider \(B \times I_n\). Let
\(V_b = \{b\} \times I_n\) for \(b \in B\) and \(V_B = \{V_b \mid b \in B\}\). Let
\(B_i = B \times \{i\}\) for \(i \in I_n\) and \(P_B = \{B_i \mid i \in I_n\}\). Since
\(n \geq 4, n \in \mathbb{N}^+[3]\). By the proof of Corollary 5.16, there are
at least two distinct LD(n,3,3)'s on \(B \times I_n\). Let
\((B \times I_n, \gamma_B, P_B, \sigma_B)\) be one of these LD(n,3,3)'s. Let
\(X' = X \setminus B_o\) and \(\sigma' = \sigma \setminus \{B_o\}\). For each \(x \in X'\), an
\((n,3,1)\)-BIBD exists, say, \(\left\{\{x\} \times I_n, \sigma_x\right\}\) since \(n = 1\) or 3
\((\text{mod } 6)\). For each of these two distinct LD(n,3,3)'s on
\(B \times I_n\) for \(B \in \mathcal{A}'\), let us form the family
\(\sigma^* = \sigma_o \cup \bigcup_{x \in X'} \sigma_x \cup \bigcup_{B \in \mathcal{A}'} \sigma_B\). We claim that \((X^*, \mathcal{B}^*, \mathcal{A}^*)\)
is a GD(n,m,3).

Let \((x,i), (y,j) \in X^*\) be any two distinct elements with
\(i \neq j\). If \(x, y \in B_o\), then \((x,i)\) and \((y,j)\) are contained
in a unique block of \(\sigma_o\). If \(x = y \notin B_o\), then \((x,i)\) and
\((x,j)\) are contained in an unique block of \(\sigma_x\). If \(x \neq y\) and
\((x,y) \notin B\) for some \(B \in \mathcal{A}'\), then \((x,y)\) is contained in an
unique block of \(\sigma^*_B\). Thus, \((X^*, \mathcal{B}^*, \mathcal{A}^*)\) is a GD(n,m,3). But
for each of these two distinct LD(n,3,3)'s on \(B \times I_n\) for
\(B \in \mathcal{A}'\) we have a distinct GD(n,m,3). Therefore, \(NGD(n,m,3,1) \geq 2^{b-1}\)
where \(b\) is the number of blocks in \(\mathcal{A}\). But
the number of pairs of points in

\[ X = \binom{m}{2} = \binom{5}{2} + (b - 1)\binom{3}{2}. \]

Thus, \( b - 1 = \frac{m^2 - m - 20}{6} \) and \( \text{NGD}(n,m,3,1) \geq 2^{b-1} \geq 2^a \) for \( m \equiv 5 \pmod{6} \).

Therefore, we have the result.

**Lemma 5.20.** If \( n \equiv 2 \pmod{6} \), then

\[ \frac{m^2 - 6m - 72}{6} \geq \text{NGD}(n,m,3,1) \geq 2 \]

for all \( m \in \mathbb{N} \) satisfying (5.11) and (5.12).

**Proof:** Let \( a = \frac{m^2 - 6m - 72}{6} \). If \( n \equiv 2 \pmod{6} \), then (5.11) and (5.12) imply that \( m \equiv 0 \pmod{6} \). By Proposition 3.23, \( n \in \text{NG}[6,3] \) and \( n \in \text{NG}[12,3] \) since \( n \geq 4 \). Thus \( \text{NGD}(n,6,3,1) \geq 1 \geq 2^a \) and \( \text{NGD}(n,12,3,1) \geq 1 \geq 2^a \). Hence we may assume that \( m \geq 18 \). Let \( m = 6m' \) for some \( m' \in \mathbb{N} \) with \( m' \geq 3 \). By Proposition 3.23, \( m' \in \text{NG}[6,3] \) since \( m' \geq 3 \).

Thus, there is a \( \text{GD}(m',6,3) \). Again by Proposition 3.23, \( n \in \text{NG}[6,3] \) since \( n \geq 4 \). By Corollary 5.16, \( n \in \text{NG}[m,3] \) and \( \text{NGD}(n,m,3,1) \geq 2^b \) where \( b \) is the number of blocks in \( \text{GD}(m',6,3) \).

Thus \( b = \frac{m^2 - 6m}{6} \) and, hence \( \text{NGD}(n,m,3,1) \geq 2^b \geq 2^a \) for \( m \geq 18 \) and \( m \equiv 0 \pmod{6} \). The proof now is complete.

**Lemma 5.12.** If \( n \equiv 5 \pmod{6} \), then
\[
NGD(n,m,3,1) \geq \frac{m^2 - 6m - 72}{6}
\]
for all \( m \in \mathbb{N} \) for which (5.11) and (5.12) hold.

**Proof:** Let \( a = \frac{m^2 - 6m - 72}{6} \). If \( n \equiv 5 \pmod{6} \), then (5.11) and (5.12) yield that \( m \equiv 0 \pmod{3} \). We have two cases.

**Case 1.** \( m \equiv 3 \pmod{6} \). For \( m = 3 \), \( n \in \text{NG}[3,3] \) by Proposition 3.22. Hence \( NGD(n,3,3,1) \geq 1 = 2^a \) for \( m = 3 \).

Assume now that \( m \geq 9 \). There is a resolvable \((m,3,1)\)-BIBD on \( m \) points since \( m \equiv 3 \pmod{6} \). Let \((X,\mathcal{A})\) be such a resolvable \((m,3,1)\)-BIBD. Let \( \mathcal{A}_1 \subseteq \mathcal{A} \) be a parallel class of blocks. Then \((X,\mathcal{A}_1,\mathcal{A}\setminus\mathcal{A}_1)\) is a GD\(\left(\frac{m}{3},3,3\right)\). Since \( n \) is odd, we have \( n \in \text{NG}[3,3] \) by Proposition 3.22. By Corollary 5.16, \( n \in \text{NG}[m,3] \) since \( n \geq 4 \). Furthermore, \( NGD(n,m,3,1) \geq 2^b \) where \( b \) is the number of blocks in \((X,\mathcal{A}_1,\mathcal{A}\setminus\mathcal{A}_1)\). It is easily seen that \( b = \frac{m(m-1)}{6} - \frac{m-1}{2} = \frac{m^2 - 4m + 3}{6} \). Thus, we have \( NGD(n,m,3,1) \geq 2^b \geq 2^a \) for \( m \equiv 3 \pmod{6} \).

**Case 2.** \( m \equiv 0 \pmod{6} \). Using the same argument as in Lemma 5.20, we have \( NGD(n,m,3,1) \geq 2^a \) for \( m \equiv 0 \pmod{6} \).

Therefore, we have the result.

From Lemmas 5.18, 5.19, 5.20, and 5.21, we have that, if \( n \) is a given positive integer, then
for all \( m \in \mathbb{N} \) for which (5.11) and (5.12) hold. Now we are ready to prove one of our main results.

**Theorem 5.22.** Let \( n \geq 3 \) be a given positive integer. Then there exist constants \( t = t_0(n) > 1 \) and \( M = M(n) \) such that

\[
N(n,m,3,l) > t^m \quad (5.14)
\]

for all \( m > M \) for which (5.11) and (5.12) hold. In particular, \( N(n,m,3,l) \to \infty \) as \( m \to \infty \) (with fixed \( n \)) in a sequence such that the quadruple \( (n,m,3,l) \) satisfies (5.11) and (5.12).

**Proof:** If \( n = 3 \), then \( GD(3,m,3) \) is TD(3,m) which has been discussed in §5.5, i.e. there are constants \( u > 1 \) and \( m_0 \) such that

\[
N(3,m,3,l) > u^m \quad (5.14)
\]

for all \( m > m_0 \).

If \( n \geq 4 \), then, since a design can be isomorphic to at most \((mn)!\) designs, we have, by (5.13),

\[
N(n,m,3,l) \geq \frac{\frac{m^2 - 6m - 72}{6}}{(mn)!} \geq 2 \quad (5.15)
\]

Note that \( m^2 \) is the dominant term on the right-hand side of
(5.15). Hence there is $m_2 = m_2(n)$ such that

$$N(n,m,3,1) > \frac{1}{2^2} m^2$$

for all $m > m_2$ for which (5.11) and (5.12) hold. Now let

$$\tilde{M} = \max(m_0, m_2(n))$$

and $t = \min(u, 2^{1/12})$. Then $t > 1$ and

$$N(n,m,3,1) > t^m$$

for all $m > \tilde{M}$ for which (5.11) and (5.12) hold.

Now let $k \geq 3$ and $\lambda$ be given positive integers. Consider

the set $D = \{d \in \mathbb{N} \mid d \text{ divides } k(k - 1)\}$ (1 and $k(k - 1)$ are

included). Recall the two numbers $s(d,k,\lambda)$ and $\tilde{N}(d,k,\lambda)$

obtained in Theorem 5.11. Let $s_1 = \min_{d \in D} s(d,k,\lambda)$ and

$$n_1 = \max_{d \in D} \tilde{N}(d,k,\lambda).$$

Then, for any $d \in D$, we have that

$$N(n,d,k,\lambda) > s_1^n$$

for all $n \in \mathbb{N}[d,k,\lambda]$ with $n > n_1$. Also

recall the two numbers $u(k)$ and $m_0(k)$ obtained in Theorem

5.17. Let $s = \min(s_1, u(k))$ and $m_1 = k(k - 1)m_0(k)$. Then

we have that

$$N(k,m,k,1) > s^m$$

(5.16)

for all $m > m_1$, and that, for any $d \in D,$

$$N(n,d,k,\lambda) > s_1^n$$

(5.17)
for all \( n \in \mathbb{N}(d,k,\lambda) \) with \( n > n_1 \).

Now let \( n,m \in \mathbb{N} \) be given positive integers such that (1.7) and (1.8) hold, and that \( nm > n_1m_1 \). Let \((m,k(k-1)) = d\). Suppose that \( TD(k,\frac{m}{d}) \) and \( GD(n,d,k,\lambda) \) exist. Let \((X,\mathcal{A})\) be a \( GD(n,d,k,\lambda) \). Let \( w: X \rightarrow \mathbb{N} \) be a weighting defined by \( w(x) = \frac{m}{d} \) for \( x \in X \). Since \( TD(k,\frac{m}{d}) \) exists, a \( GD(n,m,k,\lambda) \) exists as a result of Theorem 1.18. Since \( nm > n_1m_1 \), we have three cases, namely,

**Case 1.** \( n > n_1 \) and \( m \leq m_1 \). By (5.17), \( N(n,d,k,\lambda) > s^{n^2} \).
For each of these \( GD(n,d,k,\lambda) \)'s, we get a different \( GD(n,m,k,\lambda) \).
Thus,

\[
NGD(n,m,k,\lambda) > s^{n^2}.
\]

Let \( b_1 = s^{1/m_1^2} \). Then we have

\[
NGD(n,m,k,\lambda) > b_1^{(m_1n)^2} \geq b_1^{(mn)^2}.
\]

**Case 2.** \( n \leq n_1 \) and \( m > m_1 \). By (5.16), \( N(k,\frac{m}{d},k,\lambda) > s^{m^2} \).
For each of these \( TD(k,\frac{m}{d}) \)'s, we get a different \( GD(n,m,k,\lambda) \).
Thus,

\[
NGD(n,m,k,\lambda) > s^{m^2}.
\]

Let \( b_2 = s^{1/m_1^2} \). Then we have
NGD(n, m, k, λ) > b_2 \frac{(n,m)^2}{(nm)^2} \geq b_2 .

**Case 3.** n > n_1 and m > m_1. By (5.16) and (5.17),

N(n, d, k, λ) > s^{n^2} and N(k, \frac{m}{d}, k, l) > s^{m^2}. For each of these

GD(n, d, k, λ)'s and each of these TD(k, \frac{m}{d})'s, we get a different

GD(n, m, k, λ). Thus,

NGD(n, m, k, λ) > s^{(nm)^2} .

Now, let \( b_ο = \min(b_1, b_2, s) \). Then we derive, from these

three cases, that

NGD(n, m, k, λ) > b_ο^{(mn)^2}. 

Now as a design on a given mn-set can be isomorphic to at most

\( (mn)! \) designs, we have

\[ N(n, m, k, λ) > b_ο^{(mn)^2} / (mn)! .\]

Therefore, we get

\[ (mn)^2 - mn \log_{b_ο} (mn) \]

\[ N(n, m, k, λ) > b_ο \]

\[ (mn)^2 - mn \log_{b_ο} (mn) \]

Consider \( b_ο \). Since \( (mn)^2 \) is the dominant

term, there exist \( c > 1 \) (say \( b_ο^{1/2} = c \)) and \( ν_ο ∈ N \) such that,

for all \( mn > ν_ο \).
\[
(mn)^2 - mn \log_b (mn) > c(mn)^2.
\]

It is easily seen that both \(c\) and \(v_0\) depend on \(k\) and \(\lambda\) only. Now we may choose \(m_2, n_2 \in \mathbb{N}\) such that \(m_2 n_2 > v_0\), \(n_2 > n_1\), and \(m_2 > m_1\). Let \(\tilde{V} = m_2 n_2\). Then we have

**Theorem 5.23.** Let \(k \geq 3\) and \(\lambda\) be given positive integers. Suppose that, for any \(d \in D\), a \(\text{GD}(n,d,k,\lambda)\) exists for all \(n \in \mathbb{N}\) subject to (1.7) and (1.8), and that a \(\text{TD}(k,m)\) exists for all \(m \in \mathbb{N}\). Then there exist \(c = c(k,\lambda) > 1\) and \(\tilde{V} = \tilde{V}(k,\lambda) \in \mathbb{N}\) such that

\[
N(n,m,k,\lambda) > c(mn)^2,
\]

for all \(mn > \tilde{V}\) subject to (1.7) and (1.8). In particular, \(N(n,m,k,\lambda)\) tends to infinity as \(mn\) increases (with fixed \(k\) and \(\lambda\)) in a sequence such that the quadruple \((n,m,k,\lambda)\) satisfies (1.7) and (1.8).

By Theorem 3.16, a \(\text{GD}(n,m,3,1)\) exists for all \(n,m\) subject to (1.7) and (1.8). We also know that a \(\text{TD}(3,m)\) exists for all \(m \in \mathbb{N}\). As a corollary of Theorem 5.23,

**Corollary 5.24.** There exist \(c_3 > 1\) and \(\tilde{V}_3 \in \mathbb{N}\) such that

\[
N(n,m,3,1) > c_3(mn)^2,
\]
for all $mn > \tilde{\nu}_3$ subject to (3.13) and (3.14). In particular, $N(n,m,3,1)$ tends to infinity as $mn$ increases in a sequence such that the quadruple $(n,m,3,1)$ satisfies (3.13) and (3.14).
BIBLIOGRAPHY


