Combinatorial Network Theory

Edited by

Ding-Zhu Du
University of Minnesota
and
D. Frank Hsu
Fordham University

KLUWER ACADEMIC PUBLISHERS
DORDRECHT / BOSTON / LONDON

Library of Congress Cataloging-in-Publication Data

Combinatorial network theory / edited by Din-Zhu Du and D. Frank Hsu.
p. cm. -- (Applied optimization ; vol. 1)
ISBN 0-7923-3777-8 (HB : alk. paper)
1. Network analysis (Planning) 2. Combinatorial analysis.
I. Du, Dingzhu. II. Hsu, D. Frank (Derbiau Frank), 1948-
III. Series.
T57.85.C65 1995
511'.5--dc20 95-41542

ISBN 0-7923-3777-8

Published by Kluwer Academic Publishers,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

Kluwer Academic Publishers incorporates
the publishing programmes of
D. Reidel, Martinus Nijhoff, Dr W. Junk and MTP Press.

Sold and distributed in the U.S.A. and Canada
by Kluwer Academic Publishers,
101 Philip Drive, Norwell, MA 02061, U.S.A.

In all other countries, sold and distributed
by Kluwer Academic Publishers Group,
P.O. Box 322, 3300 AH Dordrecht, The Netherlands.

Printed on acid-free paper

Printed in the Netherlands

CONTENTS

PREFACE

Recently the interest in the interconnection of communication has grown rapidly. One of the basic problems is to design optimal interconnection networks for certain needs. For example, to minimize the communication delay and to maximize the reliability, one looks for networks with minimum diameter and maximum connectivity under certain conditions. This small book consists of five chapters:

Chapter 1: Additive Group Theory Applied to Network Topology by Y.O. Hamidoune
Chapter 2, Connectivity of Cayley Digraphs by Ralph Tindell
Chapter 3, De Bruijn Digraphs, Kautz Digraphs, and Their Generalizations by Ding-Zhu Du, Feng Cao, and D. Frank Hsu
Chapter 4, Link-Connectivities of Extended Double Loop Networks by Frank K. Hwang and Wen-Ching Winnie Li
Chapter 5, Dissemination of Information in Interconnection Networks (Broadcasting & Gossiping) by Juraj Hromkovič, Ralf Klasing, Burkhard Monien, and Regine Peine

The subject of all of the chapters is the interconnection problem. The first two chapters deal with Cayley digraphs which are candidates for networks of maximum connectivity with given degree and number of nodes. The third chapter addresses de Bruijn digraphs, Kautz digraphs, and their generalizations, which are candidates for networks of minimum diameter and maximum connectivity with given degree and number of nodes. The fourth chapter studies double loop networks, and the fifth chapter considers broadcasting and gossiping problems. Each chapter may be read independently.

All chapters emphasize the combinatorial aspects of network theory. Combinatorial network theory aspires to two goals: solving practical problems and building up beautiful mathematics. We try to meet these two challenges in this book and hope to succeed with them.

Ding-Zhu Du
D. Frank Hsu

1

ADDITIVE GROUP THEORY APPLIED TO NETWORK TOPOLOGY

Y. O. Hamidoune
CNRS, Paris
France

1.1 INTRODUCTION

In this chapter we present some basic Addition theorems and their proofs. We explain how these results apply to network topology (connectivity, superconnectivity, girth and diameter). One of our goals is to bring powerful tools from Additive group theory to networks specialists.

A network will be modeled by a relation. Of course we will have always in mind the underlying graph. We will not use undirected graphs since they may be identified with symmetric graphs. This presentation seems most appropriate for the applications from group theory. Moreover it avoids a complicated terminology frequently used in graph theory.

Motivated by the famous Waring's problem, number theorists obtained some theorems expressing lower bounds on the size of the sum of two subsets in a group. The first result of this type is an inequality proved by Cauchy (1813) and rediscovered by Davenport (1935). It states that $|A+B| \geq \min(p, |A| + |B| - 1)$, where A and B are non empty subsets of $\mathbf{Z}/p\mathbf{Z}$, and p is a prime. The motivation of Cauchy was to prove that every element of $\mathbf{Z}_p$ is the sum of k kth powers. Davenport's motivation was to prove the p-analog of the famous $(\alpha+\beta)$ conjecture due to Khintchine (1932) and solved by Mann (1942). Mann's $(\alpha+\beta)$ Theorem can be formulated as follows. Let $A, B \subset \mathbf{N}$. Then $\sigma(A+B) \geq \min(1, \sigma(A)+\sigma(B))$, where $\sigma(A) = \inf\{|A \cap [1,n]|; n \in \mathbf{N}\}$. Note that this question raised in connection with a new proof of a theorem by Hilbert asserting that for any k there is g such that every integer is a sum of g kth powers.

Ding-Zhu Du and D. Frank Hsu (eds.), Combinatorial Network Theory, 1–39.

In 1952, Mann proved the analog of his $(\alpha + \beta)$ theorem for any finite abelian group. A corollary of this result was applied to the Geometry of numbers by Kneser in 1955.

Several important contributions to Additive group theory have been obtained during the last 40 years. We mention few of them. A global Cauchy-Davenport inequality valid in any abelian group is proved by Kneser in 1955. Vosper obtained in 1956 a characterization of the cases of equality in the Cauchy-Davenport Theorem. Difficult results concerning the equality $|A + B| = |A| + |B| - 1$, where A and B are subsets of an abelian group were obtained by Kempermann (1961).

An independent work motivated by the study of the vulnerability of networks appeared recently in Combinatorics. This work is devoted to the study of the connectivity and the diameter of graphs with a transitive group of automorphisms.

It could be surprising that Additive group theory has many implications on these combinatorial problems. Actually all these questions for Cayley graphs have been more or less considered in Additive group theory. For this reason several facts from this theory have been rediscovered recently in connection with network vulnerability. The Cauchy-Davenport Theorem is rediscovered by the author (1977) in an equivalent form saying that the connectivity of a Cayley graph with a prime order is optimal. In 1970, Behzad and al conjectured that the minimum order of directed graph with girth g and degree d is $1 + d(g - 1)$. They were certainly unaware of a result of Shepherdson (1947) stating that this result holds for loop networks. In 1987, Boesch and Tindell rediscover a special case of the corollary of the finite $(\alpha + \beta)$ -Theorem mentioned above. The motivation of Boesch and Tindell was to obtain a necessary and sufficient condition for an undirected loop network to be with optimal connectivity.

Recently networks specialists become interested in constructing loop networks with given degree and minimum diameter. This question was considered in number theory in an equivalent formulation. It is known as the minimum base with a given order.

Our plan in this chapter is to introduce basic results from Additive group theory and to apply them to networks. Some of these applications are new. For example, the theory of atoms provides some properties of minimum cutsets. Unfortunately this theory does not apply to other cuts. We show here that such an information is contained in the finite $(\alpha+\beta)$ Theorem and Kneser's Theorem.

The diameter of the loop network defined by the k th powers was studied in number theory. We give here a nice method due to Chowla, Mann and Straus to prove that this number is bounded by $[k/2]+1$, in a prime order using Vosper's Theorem. The determination of superconnected loop networks, i.e. where every minimum cutset is of the $\partial^+(x)$ or $\partial^-(x)$ for some node x, received a lot of attention. We show how Vosper's Theorem implies easily that a loop network of a prime order not defined by an arithmetic progression is superconnected.

We prove Kneser's Theorem and mention some of its applications to abelian Cayley graphs. We give an outline of Kempermann critical pair theory and mention how to use it in order to characterize superconnected loop networks.

In the last section, we deal with the minimum cardinality of a base with given order and mention its connection with the minimum diameter of a loop network with a given degree.

1.2 BASIC NOTIONS

1.2.1 Preliminaries from Group Theory.

We shall assume some familiarity with the notion of a subgroup, of a coset and of a homomorphism. We use only elementary facts from group theory. We summarize them below for the commodity of the reader. We advice him to prove the following lemmas as exercises using only the definitions, which may be found in any book of group theory.

The cardinality of a set V will be denoted by $|V|$, if V is infinite we write $|V| = \infty$.

Let G be a group with a law written multiplicatively and let A and B be subsets of G. We write $A^{-1} = \{x^{-1} : x \in A\}$. The product of A and B is defined as $AB = \{xy : x \in A \text{ and } y \in B\}$. Let $x \in G$, we write xA for $\{x\}A$ and Ax for $A\{x\}$. In the case of abelian groups we will use the additive notations. In particular we write $A + B = \{x + y : x \in A \text{ and } y \in B\}$, etc.

Lemma 1.2.1 *Let G be a group containing three subsets A, B and C. Then $A(BC) = (AB)C$ and $(AB)^{-1} = B^{-1}A^{-1}$.*

The proof is immediate.

The *product* of A with itself k times will be denoted by A^k. In the additive notations, we use kA for $A + A + \cdots + A$, k times.

Let G be a group and let $x \in G$. The *left translation* with respect to x is the mapping $\gamma_x : G \longrightarrow G$, where $\gamma_x(y) = xy$, for any $y \in G$.

Lemma 1.2.2 *Let G be a group containing an element x and two subsets A and B. Then γ_x is a bijection from G onto G. Moreover $\gamma_x(A) = xA$. In particular $|xA| = |A|$, $x(A \cap B) = (xA) \cap (xB)$ and $x(A \backslash B) = (xA) \backslash (xB)$.*

The proof is immediate.

Lemma 1.2.3 *Let G be a group containing two non empty subsets A and B. Then $|AB| \geq |A|$. In particular $AB = A$ if and only if $AB \subset A$.*

The proof is immediate.

The above three lemmas will be applied without any reference.

Let G be a group containing an element x and a subset S and let H be a subgroup of G. We recall that xH is called a *left coset* of H. The *subgroup generated* by S is by definition the smallest subgroup of G containing S. We shall denote it by $< S >$.

We use the following lemmas.

Lemma 1.2.4 *Let G be a group containing a finite nonempty subset A. Then A is a subgroup if and only if $AA = A$.*

The proof is an easy exercise.

Lemma 1.2.5 *Let G be a group containing two finite subsets A and S. Then the following conditions are equivalent.*

(i) $AS = A$

(ii) $A < S >= A$

(iii) A *is the union of left cosets of* $< S >$.

The proof is left as an exercise.

We shall denote the ring of integers modulo n by $\mathbf{Z}_n$. The set of units of $\mathbf{Z}_n$ will be denoted by $\mathbf{Z}_n^*$.

Lemma 1.2.6 *Let* $n \in \mathbf{N}$ *and let* $x \in \mathbf{Z}_n$. *Then* $x \in \mathbf{Z}_n^*$ *if and only if* $< x >= \mathbf{Z}_n$, *where* $< x >$ *is the additive subgroup generated by* x.

Lemma 1.2.7 *Let* p *be a prime number. Then* $\mathbf{Z}_p$ *is a field. In particular,* $\mathbf{Z}_p^*$ *is a group with respect to multiplication.*

In the proof of Kneser's Theorem we will use the notion of factor group. We use the following well-known result.

Proposition 1.2.8 *Let* f *be an endomorphism of a finite group. Then* $|Im(f)| \cdot |Ker(f)| = |G|$.

In the last section, we shall use the structure of finite abelian groups. We summarize it below. Let G be an abelian group containing subgroups G_1, G_2, $\cdots$, G_k ($k \in \mathbf{N}$). Recall that G is said to be a *direct sum* of the family $\{G_1, G_2, \cdots, G_k\}$ if every element x of G has a unique expression $x = x_1 + x_2 + \cdots + x_k$, where $x_i \in G_i$, $1 \leq i \leq k$. This holds if and only if G is isomorphic to $G_1 \times G_2 \times \cdots \times G_k$. The following lemma is well-known.

Lemma 1.2.9 *Let* $k \in \mathbf{N}$ *and let* G *be an abelian group containing subgroups* $G_1, G_2, \cdots, G_k$. *Then* G *is a direct sum of* $\{G_1, G_2, \cdots, G_k\}$ *if and only if* $G = G_1 + G_2 + \cdots + G_k$ *and for every* $1 \leq i \leq k-1$, $G_{i+1} \cap (G_1 + G_2 + \cdots + G_i) = \{0\}$.

Let p be a prime number. A finite group G is said to be a p-group if there is $s \geq 1$ such that $|G| = p^s$. Let G be a finite abelian group. Following Lang, we write $A(p) = \{x : |< x >| \text{ is a power of } p\}$. The following result is well-known.

Theorem 1.2.10 *Let G be an abelian group and let $P = \{p : p \text{ is a prime and } A(p) \neq \{0\}\}$. For any $p \in P$, $A(p)$ is a p-group. Moreover G is a direct sum of the family $\{A(p); p \in P\}$.*

The structure of abelian p-groups is given by the following result.

Theorem 1.2.11 *Let G be an abelian p-group. Then G is a direct sum of cyclic p-groups.*

1.2.2 Networks Terminology

Let V be a set. The graph of the diagonal relation will be denoted by $\Delta(V)$. We have $\Delta(V) = \{(x, x) : x \in V\}$.

We recall some classical definitions from Set theory. A *relation* on a set V is an ordered pair (V, E), where E is a subset of $V \times V$. The set E will be called the *graph* of Γ. The elements of E will be called *arrows* or *arcs*. A relation will be sometimes called a *network*. In this case the points are usually called *nodes*. From now on we identify a relation with its graph and call the points vertices. The usual operations defined on relations (e.g., composition ...) will be applied to graphs.

Let Γ be a graph on a set V and let A be a subset of V. The *image* of A under Γ will be denoted by $\Gamma(A)$. We recall that

$$\Gamma(A) = \{y : \exists x \in A, (x, y) \in E\}.$$

We write $\partial_\Gamma(A) = \Gamma(A) \backslash A$. When the context is clear we write ∂ instead of ∂_Γ.

Let $x \in V$, we write $\Gamma(x) = \Gamma(\{x\})$ and $\partial(x) = \partial(\{x\})$. The *degree* of x is defined as $d_\Gamma(x) = |\partial(x)|$. If all points of V have the same degree, the graph will be called regular. Let Γ be a regular graph. The common degree of all points of Γ will be called the degree of Γ and will be denoted by $d(\Gamma)$. According to our definition, the degree of a point x with respect to $\Gamma \cup \Delta(V)$ is the same as $d_\Gamma(x)$. In others terms loops are not counted in the degree. However we will not exclude them in developing the theory. It is even desirable to add them in order to simplify some proofs and some notations.

Let $\Gamma = (V, E)$ be a graph. The *inverse* graph of Γ is the graph $\Gamma^- = (V, E^-)$, where $E^- = \{(x, y) : (y, x) \in E\}$.

A graph is said to be *locally finite* if every point has a finite degree. A graph will be called *finite* if its set of points is finite.

A graph Γ on a set V is said to be *connected* if for every $A \subset V$, such that $A \neq \phi$ and $A \neq V$, $\Gamma(A) \not\subset A$.

From now on, all graphs are assumed to be locally finite.

The *connectivity* of a graph $\Gamma = (V, E)$, denoted by $\kappa(\Gamma)$, is defined as follows.

$$\kappa(\Gamma) = min\{|\partial(F)| : |F| = 1 \text{ or } \phi \neq F \cup \Gamma(F) \neq V\}.$$

Lemma 1.2.12 *Let $\Gamma = (V, E)$ be a graph. Then*

(i) $\kappa(\Gamma \cup \Delta(V)) = \kappa(\Gamma)$.

(ii) $\kappa(\Gamma) \leq \min\{d(x) : x \in V\}$.

The proof is easy.

A subset F such that $\kappa(\Gamma) = |\partial(F)|$ and $F \cup \Gamma(F)$ is a proper subset of V is called a *fragment.*

Lemma 1.2.13 *Let $\Gamma = (V, E)$ be a graph. Then $\kappa(\Gamma)$ is the maximal integer k such that for any nonempty subset F of V, $|F \cup \Gamma(F)| \geq \min(|V|, |F| + k)$.*

The proof follows easily from the definitions.

Lemma 1.2.14 *Let $\Gamma = (V, E)$ be a regular graph. Then the following conditions are equivalent.*

(i) $\kappa(\Gamma) = d(\Gamma)$.

(ii) For any nonempty subset F of V,

$$|F \cup \Gamma(F)| \geq \min(|V|, |F| + d(\Gamma)).$$

The proof is easy.

Lemma 1.2.15 *Let Γ be a finite graph. The following conditions are equivalent.*

(i) Γ is connected.

(ii) For any two points x and y, there is a path from x to y in the graph of Γ.

(iii) $\kappa(\Gamma) \geq 1$.

Let Γ be a graph on a set V and let $A \subset V$. The *subgraph* induced on A is by definition $\Gamma[A] = (A, E \cap (A \times A))$. A subset T is said to be a *cutset* of Γ if $\Gamma[V \backslash T]$ is not connected. It is clear that $\partial(F)$ is a cutset if $F \neq \phi$ and $F \cup \Gamma(F) \neq V$. Let A and T be nonempty subsets. We will say that T is a *fundamental cutset* with *support* A if $\partial(A) = T$ and $A \cup T \neq V$. The following lemma shows how to construct all cutsets from the fundamental cutsets.

Lemma 1.2.16 *Let $\Gamma = (V, E)$ be a graph and let $T \subset V$. Then T is a cutset of Γ if and only there is a fundamental cutset $T' \subset T$ and a support F of T' such that $F \not\subset T$ and $(V \setminus (F \cup T')) \not\subset T$.*

The proof is easy.

Lemma 1.2.17 *Suppose that $\Gamma \cup \Delta(V) \neq V \times V$. Then every minimal cutset is a fundamental cutset. Moreover $\kappa(\Gamma)$ is the minimal cardinality of a cutset of Γ.*

The proof is easy.

A cutset T is said to be a *minimum cutset* if $|T| = \kappa(\Gamma)$.

Lemma 1.2.18 ([13]) *Let Γ be a finite graph. Then $\kappa(\Gamma) = \kappa(\Gamma^-)$.*

The proof is left to the reader.

Let $\Gamma = (V, E)$ be a regular finite graph. The graph Γ is said to be *superconnected* if $\kappa(\Gamma) = d(\Gamma)$ and if for every minimum cutset of Γ, there is $x \in V$ such that $T = \partial(x)$ or $T = \partial^-(x)$.

NOTICE. There is no standard terminology in Graph theory. The reader should take care before applying results from this area. The connectivity is called sometimes strong connectivity and in particular strongly connected should be replaced by connected. They use also the word outdegree for our notion of degree. In graph theory some authors use directed graph (or digraph) instead of graph. The definition of graph we use is contained in Bourbaki. It is standard in Mathematics, except some parts of graph theory.

A graph Γ is said to be *point-transitive* if its group of automorphisms acts transitively on its points. The following lemma is well-known and easy.

Lemma 1.2.19 *Let Γ be a point-transitive graph on a set V. Then Γ is regular. Moreover $d(\Gamma) = d(\Gamma^-)$, if V is finite.*

Let us now define the notion of *diameter* of a graph. We shall make this without reference to the notion of a path.

Let Γ be a graph on a set V. We recall that Γ^k is the relation obtained by composing Γ with itself k times. For any $x \in V$, we have $\Gamma^k(x) = \Gamma(\Gamma(\ldots(\Gamma(x))\cdots)$, k times. We write $\Gamma^0 = \Delta(V)$.

Let x and y be two points of V. The distance from x to y is by definition $dist_\Gamma(x,y) = \min\{k : y \in \Gamma^k(x)\}$, where $\min \phi = \infty$. The diameter of Γ is by definition $\rho(\Gamma) = \max\{\text{dist}_\Gamma(x,y) : x,y \in V\}$.

Notice that the the diameter is not affected by the addition of loops.

Lemma 1.2.20 *Let Γ be a graph on a set V and let x and y be two points of V. Then dist (x,y) is the minimal length of a path from x to y in the graph of Γ.*

The proof is easy.

Let $\Gamma = (V,E)$ be a graph. The *girth* of Γ is by definition $\eta(\Gamma) = 1 + \min\{\text{dist}(y,x) : (x,y) \in E\backslash\Delta(V)\}$.

Notice that the girth is not affected by the addition of loops.

Lemma 1.2.21 *Let Γ be a finite graph on a set V. Then $\eta(\Gamma)$ is the minimal length of a (directed) cycle in the graph of $\Gamma\backslash\Delta(V)$.*

The proof is easy.

We shall use these notions only in the case of point-transitive graphs. The following lemma shows that these notions become more simple in this case.

Lemma 1.2.22 *Let Γ be a point-transitive graph on a set V and let $v \in V$. Then*

(i) $\rho(\Gamma) = \max\{dist_\Gamma(v,x) : x \in V\}$.

(ii) $\eta(\Gamma) = \min\{k : v \in \Gamma^{k-1}(\partial(v)\}$.

The proof is easy.

1.2.3 Cayley Graphs

An important class of point-transitive graphs is the class of Cayley graphs defined below.

Let G be a group and let S be a subset of G. The *Cayley graph* on G defined by S is the graph $\Lambda(G,S) = (G,E)$, where $E = \{(x,y) : x^{-1}y \in S\}$.

Lemma 1.2.23 *Let G be a group containing a subset S and let $\Gamma = \Lambda(G,S)$ For every $F \subset G$, $\Gamma(F) = FS$ and $\partial(F) = (FS)\backslash F$.*

The proof follows from the definitions.

Lemma 1.2.24 *Let G be a group and let B be a finite subset of G. Then $\kappa(\Lambda(G,B))$ is the maximal integer k such that for any nonempty subset F of G,*

$$|F(B \cup \{1\})| \geq \min(|G|, |F| + k).$$

The proof follows from Lemmas 1.2.23 and 1.2.2.

Lemma 1.2.25 *Let G be a group and let B be a finite subset of G. Then*

$$\kappa(\Lambda(G, B \cup \{1\})) = |B \cup \{1\}| - 1$$

if and only if for all $A \neq \phi$,

$$|A(B \cup \{1\})| \geq \min(|G|, |A| + |B \cup \{1\}| - 1).$$

The proof follows from Lemmas 1.2.14 and 1.2.23.

Lemma 1.2.26 *Let G be a finite group and let $B \subset G$. Then*

(i) $\rho(\Lambda(G, B)) = \min\{k : (B \cup \{1\})^k = G\}$.

(ii) $\eta(\Lambda(G, B)) = \min\{k : 1 \in (B \setminus \{1\})(B \cup \{1\})^{k-1} = G\}$.

The proof follows from the definitions and Lemma 1.2.22

Lemma 1.2.27 *Let G be a finite group and let B be a subset of G. Then $\Lambda(G, B)$ is connected if and only if $G =< B >$.*

The proof is easy.

1.3 THE FINITE $(\alpha + \beta)$-THEOREMS

In subsection 1.3.1, we introduce the Dyson's transform and give its basic properties. We use it to prove the Cauchy-Davenport Theorem. This proof is closely related to that given in [46]. Note that several other proofs exist. In particular the reader may found an elegant and short proof in [8].

In subsection 1.3.2, we prove the Mann finite $(\alpha + \beta)$ Theorem and its additive consequences. The proof presented here is closely related to Mann's proof [36].

In subsection 1.3.3, we apply the finite $(\alpha + \beta)$-Theorem and its corollaries to the study of the cutsets in Cayley graphs. However, we think that this result can be used to prove other interesting properties of Cayley networks and advice the reader to search more applications for this result.

In subsection 1.3.4, we present two criteria due to Shepherdson and Scherk implying the Cauchy-Davenport inequality for a general abelian group. We present a corollary due to Shepherdon which determines the minimal order of Cayley graph with given degree and girth. The proofs given here for Shepherdon and Scherck are different from the orignal ones which use a trnsform due to Davenport.

1.3.1 The Cauchy-Davenport Theorem

The main result of this subsection is the Cauchy-Davenport Theorem. Let us define the Dyson's *transform.*

Let G be an abelian group containing two nonempty subsets A and B and let $e \in G$. The Dyson's e-transform of (A, B) is (A^*, B^*), where $A^* = A \cup (e + B)$ and $B^* = B \cap (A - e)$. The basic properties of the Dyson's transform are the following.

Lemma 1.3.1 *Let G be an abelian group containing two nonempty subsets A and B and let $e \in G$. Let $A^* = A \cup (e + B)$ and let $B^* = B \cap (A - e)$. Then*

(i) $A^* + B^* \subset A + B$.

(ii) $|A^*| + |B^*| = |A| + |B|$.

Proof. We have clearly

$$A^* + B^* = A \cup (e+B) + B \cap (A-e) \subset (A+B) \cup ((e+B) + (A-e)) \subset A+B.$$

We have, using Lemma 1.2.2,

$$\begin{aligned} & |A^*|+|B^*|=|A \cup (e+B)|+|B \cap (A-e)| \\ = \; & |A| + |e+B| - |A \cap (e+B)| + |B \cap (A-e)| \\ = \; & |A| + |B|. \end{aligned}$$

□

Theorem 1.3.2 (Cauchy [5], Davenport [8]) *Let p be a prime number and let A, B be nonempty subsets of $\mathbf{Z}_p$. Then $|A + B| \geq \min(p, |A| + |B| - 1)$.*

Proof. The proof is by induction on $|B|$. The result is obvious for $|B| = 1$. Suppose the result is proved for all B' with $|B'| < k$, where $k = |B| \geq 2$. Take $b \in B$ and put $S = B - b$. We have clearly $0 \in S$ and $< S >= \mathbf{Z}_p$.

Let A be a subset of G. The inequality of the theorem holds trivially if $|A| = 1$. Assume $|A| \geq 2$. Suppose first that for every $a \in A$, $a + S \subset A$. Therefore $A + S \subset A$. By Lemma 1.2.3, $A + S = A$. By Lemma 1.2.6, $|A| \geq |< S >| = p$. In this case the inequality of the theorem is obviously verified.

Suppose now that there exists $a \in A$ such that $(a + S) \backslash A \neq \phi$. Put $A^* = A \cup a + S$ and $S^* = S \cap (A - a)$. Since $(a + S) \not\subset A$, we have using Lemma 1.2.3, $|S^*| < |S|$. Clearly $0 \in S$. By the induction hypothesis we have

$$|A^* + S^*| \geq \min(p, |A^*| + |S^*| - 1).$$

By Lemma 1.2.12, we have $|A + S| \geq \min(p, |A| + |S| - 1)$. But clearly $|S| = |B|$ and $|A + S| = |A + B|$. This last remark completes the proof of the theorem. □

Theorem 1.3.2 is the p-analog of the $(\alpha + \beta)-$Theorem. According to Lemma 1.2.24, Theorem 1.3.2 is equivalent to the following result rediscovered in 1977.

Theorem 1.3.3 ([13]) *Let p be a prime number and let B be a nonempty subset of $\mathbf{Z}_p$. Then $\kappa(\Lambda(\mathbf{Z}_p, B)) = |B \backslash \{0\}|$.*

1.3.2 Mann's Theorem

The following lemma is well-known.

Lemma 1.3.4 *Let A, B be finite subsets of a group G such that $AB \neq G$. Then $|A| + |B| \leq |G|$.*

Proof. Let $x \in G \backslash AB$. We have clearly $xB^{-1} \cap A = \phi$. It follows

$$|A| + |B| = |A| + |B^{-1}x| = |A \cup B^{-1}x| \leq |G|. \quad \square$$

Proposition 1.3.5 (Mann, [34, 36]) *Let G be a finite abelian group and let A, B be subsets of G such that $0 \notin A + B$. There is a subgroup H of G and a subset W with the following properties.*

(i) $A \subset W$

(ii) $W + B = G \backslash H$

(iii) $|W| - |A| = |W + B| - |A + B|$.

Proof. The proof is by induction on $k(A, B) = |G| - |A + B|$. If $k(A, B) = 1$, the theorem holds trivially with $W = A$ and $H = \{0\}$. Suppose $k \geq 2$. Put $D = G \backslash (A + B)$. Since $0 \in D$, we have clearly $D \subset D + D$. If $D + D = D$ then by Lemma 1.2.5, D is a subgroup, in this case the theorem holds trivially with $W = A$ and $H = D$. Suppose the contrary and choose $(r, s, a, b) \in D \times D \times A \times B$ such that $r + s = a + b$. Put $A^* = (a - D) \cap (D - B)$ and $C = A \cup A^*$.

We begin by showing the equality

$$(A^* + B) \cap D = D \cap (a - A^*) \tag{1.1}$$

We have clearly $a - A^* = D \cap (a + B - D)$. Let $x \in (A^* + B) \cap D$. Choose $(v, u) \in B \times A^*$ such that $x = u + v$. Since $u \in (a - D)$, we have $x \in a + B - D$. This shows the first inclusion.

Let $x \in (a - A^*) \cap D = D \cap (a + B - D)$. Choose $v \in B$ and $y \in D$ such that $x = a + v - y$. Now $a - y = x - v \in D - B$. Clearly $a - y \in (a - D)$. Therefore $a - y \in A^*$. It follows that $x \in A^* + B$. This shows the second inclusion.

Let us show that $A^* \cap A = \phi$. Suppose on the contrary that there exists $u \in A \cap A^*$. It follows that $u \in A \cap (D - B)$, a contradiction. From (1), we get $|(A^* + B) \cap D| = |D \cap (a - A^*)|$. Hence

$$|(A^* + B) \cap D| = |(a - D) \cap A^*| = |(a - D) \cap (D - B)| = |A^*|. \tag{1.2}$$

Therefore

$$|C| - |A| = |A^*| = |C + B| - |A + B| \tag{1.3}$$

Now we have clearly $a - r \in A^*$. It follows that $a - r + b \in (A^* + B) \backslash (A + B)$. Therefore $|G| - |A + C| < |G| - |A + B|$. We have also $0 \notin C + B$, since otherwise there is $t \in B$ and $q \in D$, such that $q - r \in A$, a contradiction.

By the induction hypothesis, there exists a subgroup H and a subset W such that

$$C \subset W,\ C + W = G \backslash H \text{ and } |W| - |C| = |C + W| - |C + B| \tag{1.4}$$

By (1.3) and (1.4), we have $|W| - |A| = |W + B| - |A + B|$, which proves the theorem. □

The condition $0 \notin A+B$ may be replaced by $x \notin A+B$, where x is an arbitrary element of G. However the general case follows from the case $0 \notin A + B$.

Theorem 1.3.6 (Mann, [34, 36]) *Let G be a finite abelian group and let A, B be subsets of G such that $c \notin A + B$. There is a subgroup H of G and a subset W with the following properties.*

(i) $A \subset W$ and $W + B = G\backslash(c + H)$

(ii) $|W| - |A| = |W + B| - |A + B|$.

Proof. Let $B' = B - c$. Clearly $0 \notin A + B'$. By Theorem 1.3.4, there are a subgroup H and a subset W such that

$$A \subset W \text{ and } W + B' = G\backslash H \tag{i}$$

$$|W| - |A| = |W + B'| - |A + B'|. \tag{ii}$$

The result follows now since $W + B = W + B' + c = G\backslash(c + H)$, $|W + B| = |W + B'|$ and $|A + B| = |A + B'|$. □

We will refer to Theorem 1.3.6 as the finite $(\alpha + \beta)-$Theorem.

Corollary 1.3.7 (Mann, [34, 36]) *Let G be a finite abelian group and let A, B be nonempty subsets of G such that $A + B \neq G$. There exists a subgroup H such that $H + B \neq G$ and $|A + B| \geq |A| + |B + H| - |H|$.*

Proof. Suppose $A + B \neq G$ and choose $x \in G\backslash(A + B)$. By Theorem 1.3.6, there are a subgroup H and a subset $W \supset A$ with the following property.

$$W + B = G\backslash(x + H) \text{ and } |A + B| - |A| = |W + B| - |W|. \tag{1.5}$$

Clearly, $|W + B| = |G| - |x + H| = |G| - |H|$. Since $W + H + B = W + B + H = (G\backslash(x+H)) + H \neq G$, we have by Lemma 1.3.4, $|G| \geq |W| + |B + H|$. It follows from (1) that $|A + B| - |A| \geq |W + B| - |W| \geq |B + H| - |H|$.