AN ABSTRACT OF THE THESIS OF

ROGER LEON HIGDEM (Name) for the DOCTOR OF PHILOSOPHY (Degree)

in MATHEMATICS (Major) presented on August 14, 1970 (Date)

Title: SUMS OF SUBSETS OF CERTAIN ALGEBRAIC SYSTEMS

Signature redacted for privacy.

Abstract approved: R. D. Stalley

In this thesis we investigate the extension of certain theorems of additive number theory to three algebraic systems. A generalization of a theorem by Cauchy and Davenport on the cardinality of the sum of two sets of residue classes is given. We obtain and compare estimates for the order of a basis set of n-dimensional lattice points. These estimates are obtained using the best density inequality theorems available for the densities of Schnirelmann, Kasch and Kvarda. Finally additive number theory is extended to Boolean algebra. First, cardinality conditions are found for a given element to be in a sum (product) of sets. Next, the cardinality of the sum (product) of two sets is investigated. Finally, a modified sum is studied and some conjectures are made.

Sums of Subsets of Certain Algebraic Systems

by

Roger Leon Higdem

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

June 1971

APPROVED:

Signature redacted for privacy.

Professor of Mathematics

in charge of major

Signature redacted for privacy.

Acting Chairman of Department of Mathematics

Signature redacted for privacy.

Dean of Graduate School

Date thesis is presented August 14, 1970

Typed by Clover Redfern for Roger Leon Higdem

ACKNOWLEDGMENTS

To Mary who helped and Dane who tried. To Dr. Robert D. Stalley whose time and assistance made the writing of this thesis possible.

TABLE OF CONTENTS

SUMS OF SUBSETS OF CERTAIN ALGEBRAIC SYSTEMS

CHAPTER I

INTRODUCTION

The general problem of additive number theory may be stated as "the study of the properties of integers which involve the operation of addition." A more specific definition is given by Hardy and Wright [13, p. 273]:

> The general problem of [additive number] theory may be stated as follows. Suppose that A or $a_1, a_2, a_3, \ldots$ is a given system of integers. Thus A might contain all the positive integers, or the squares, or the primes. We consider all possible representations of an arbitrary positive integer n in the form
>
> $$n = a_{i_1} + a_{i_2} + \ldots + a_{i_s},$$
>
> where s may be fixed or unrestricted, the [integers] a may or may not be necessarily different, and order may or may not be relevant, according to the particular problem considered. We denote by $r(n)$ the number of such representations. Then, what can we say about $r(n)$? For example, is $r(n)$ always positive? Is there always at any rate one representation for every n?

The latter definition can be criticized for being too restrictive. For instance it is not possible to specify one form for some of the integers a and another form for the others. This definition leads to a description of our work.

In this thesis we study the extension of the following general problem of additive number theory to certain algebraic systems. "Let $A_1, A_2, \ldots, A_k$ be sets of nonnegative integers and let $S = \{n \mid n = a_1+a_2+\ldots+a_k,\ a_i \in A_i,\ i = 1, 2, \ldots, k\}$. Study the distribution of S and its relation to k." In Chapter 2 we present a generalization of a well known theorem of additive number theory where $k = 2$ and the elements of A_1 and A_2 are residue classes. In Chapter 3 we let the elements of $A_1 = A_2 = \ldots = A_k$ be n-tuples of nonnegative integers and find estimates for the lower bound for k so that S is the set of all such n-tuples. In Chapter 4 we extend the general problem to Boolean algebras and study two problems in detail, one where $k = 2$ and one where k is an arbitrary fixed integer. Finally, in Chapter 5 we further extend the Boolean algebra investigation by modifying the definition of the sum for $k = 2$. Since each chapter concerns a different algebraic system, we leave the detailed introduction to our work to the particular chapters.

We further describe our contributions in this thesis as follows. In Chapter 2 we prove a new generalization of the Cauchy-Davenport inequality. In Chapter 3 we obtain new conditions for a set to be a basis and obtain new bounds for the order of a basis. In Chapters 4 and 5 we develop a new additive theory where essentially none exists at present.

Each chapter is self contained except that Chapter 5 uses the

definitions and some of the theorems of Chapter 4. Unsolved problems are mentioned in the course of the chapters.

Definitions, lemmas and theorems are numbered consecutively in each chapter. Numbered equations within each theorem begin with (1). We use Greek letters for real variables and Latin letters for integer variables unless otherwise specified. We use $X \subset Y$ to mean that X is contained in Y. In the event we want to show proper containment we will write $X \subsetneq Y$.

Finally, any theorem which is not attributed to another source by a reference or statement can be assumed to be the author's.

There are three standard reference texts, namely those of H.-H. Ostmann [21], H. B. Mann [19], and H. Halberstram and K. F. Roth [12].

CHAPTER II

SUMS OF SUBSETS OF RESIDUE CLASSES

Section 2-1. Introduction.

Definition 2.1. Let $\overline{g}$ be defined by the equation $\overline{g} = \{x \mid x \equiv g \pmod{m}\}$.

Definition 2.2. Let $(G, +)$ be the additive group of residue classes modulo m.

Note that $G = \{\overline{g} \mid 0 \leq g < m\}$. Note also that any finite cyclic group is isomorphic to an additive group of residue classes modulo m, thus the theory of this chapter has this broader interpretation.

Definition 2.3. Let A and B be nonempty subsets of G. The sum $A + B$ of A and B is given by $A + B = \{a + b \mid a \in A, b \in B\}$.

Definition 2.4. For $X \subset G$, let $|X|$ denote the cardinality of X.

Definition 2.5. Let (s, t) denote the greatest common divisor of s and t.

In 1935 H. Davenport [6] proved the following theorem but

reported that Cauchy had given a proof in 1813.

Theorem 2.6 (Cauchy-Davenport). If m is a prime, then $|A + B| \geq \min \{m, |A| + |B| - 1\}$.

In 1937 I. Chowla [4] extended Theorem 2.6 to composite m with the restriction that $\overline{0} \in B$ and $(b, m) = 1$ for each $\overline{b} \in B$, $\overline{b} \neq \overline{0}$. H. Mann [18] gave another proof of Chowla's result in 1952. In 1937 S. Pillai [22] generalized Theorem 2.6 in a different direction by showing that for m arbitrary, $|A+B| \geq \min_{\max} \{m/d, |A|+|B|-1\}$, where $d = \max \{(m, b-b') | \overline{b}, \overline{b}' \in B, \overline{b} \neq \overline{b}'\}$. Several writers have extended Theorem 2.6 to Abelian groups.

In Section 2-2 we generalize Chowla's result in $(G, +)$. The method of proof is different from that used by Chowla or Mann.

Section 2-2. A Generalization of a Theorem of Cauchy and Davenport.

Theorem 2.7. Let $\overline{0} \in B$. If $|B| > 1$, let $(m, b) = d$ for all $\overline{b} \in B$, $\overline{b} \neq \overline{0}$. If $|B| = 1$, let $d = 1$. Let $A(d) = \{r | 0 \leq r < d, r \equiv a \pmod d, \overline{a} \in A\}$ and $k = |A(d)|$. Then $|A + B| \geq \min \{km/d, |A|+|B|-1\}$.

Proof. We use induction on $|B|$.

If $|B| = 1$, then $B = \{\overline{0}\}$ and so $A + B = A$. Thus,

$$|A + B| = |A| = |A| + |B| - 1.$$

Hence we suppose $|B| = r$, $1 < r \leq m$, and assume the theorem valid for all sets B where $1 \leq |B| < r$. We have two cases.

Case 1. $A + B = A$.

Let $\overline{a} \in A$, $\overline{b} \in B$ and $\overline{b} \neq 0$. Then $\overline{a} + \overline{b} \in A$, and so $\overline{c}_1 \in A$ where $c_1 = a + b$. Similarly $\overline{c}_2 \in A$, where $c_2 = a + 2b = c_1 + b$, and by induction on n we have $\overline{c}_n \in A$ where $c_n = a + nb = c_{n-1} + b$, and where $n \geq 1$ is arbitrary.

By a well known result of number theory, if $h \equiv a \pmod{d}$, then

$$a + bx \equiv h \pmod{m}$$

has a solution and so is satisfied by a positive integer $x = n$. Thus $h \equiv c_n \pmod{m}$ and so $\overline{h} = \overline{c}_n \in A$. For $r \in A(d)$ let

$$A_r = \{\overline{x} | \overline{x} \in A,\ x \equiv r \pmod{d}\}.$$

If $h_j = r + jd$, then $h_j \equiv r \pmod{d}$ and so $\overline{h}_j \in A$. Hence $\overline{h}_j \in A_r$ and so $A_r = \{\overline{h}_j | j \text{ is an integer}\}$. If $sd = m$, then $h_j \equiv h_{j+s} \pmod{m}$ and $h_{j_1} \neq h_{j_2}$ if $1 \leq j_1 < j_2 \leq s$. Hence

$$A_r = \{\overline{h}_j | 1 \leq j \leq s\},$$

and so $|A_r| = s = m/d$. Also, since $A_r \subset A$ then $\{A_r | r \in A(d)\}$

is a partition of A. Finally

$$|A + B| = |A| = \sum_{r \in A(d)} |A_r| = \frac{km}{d},$$

and the theorem follows for Case 1.

Case 2. $A + B \neq A$.

We use a set construction of F. Dyson [7]. Since $\overline{0} \in B$, we have $A \subset A + B$, and so there exists $\overline{a}_0 \in A$ such that $\overline{a}_0 + \overline{b} \notin A$ for some $\overline{b} \in B$. Let

$$B' = \{\overline{b} \mid \overline{b} \in B,\ \overline{a}_0 + \overline{b} \notin A\},$$

$$A' = \{\overline{a}_0 + \overline{b} \mid \overline{b} \in B'\},$$

$$A_1 = A \cup A',$$

and

$$B_1 = B \setminus B'.$$

Since $\overline{0} \in B_1$ and $|B_1| < |B|$ we have by the induction hypothesis that

$$(1) \qquad |A_1 + B_1| \geq \min \{k_1 m/d_1,\ |A_1| + |B_1| - 1\},$$

where d_1 and k_1 are defined for B_1 and A_1 just as d and k are defined for B and A. Since $|B_1| = |B| - |B'|$,

$|A_1| = |A| + |A'|$ and $|A'| = |B'|$, then $|A_1| + |B_1| = |A| + |B|$. If $|B_1| > 1$, then $d_1 = d$ since $B_1 \subset B$, and $k_1 \geq k$ since $A \subset A_1$. If $|B_1| = 1$, then $k_1/d_1 = 1 \geq k/d$. Hence, from the inequality (1) we have

$$|A_1 + B_1| \geq \min \{km/d, |A| + |B| - 1\}.$$

The induction is completed by showing $A_1 + B_1 \subset A + B$. Suppose $\bar{a}_1 \in A_1$ and $\bar{b}_1 \in B_1$. If $\bar{a}_1 \in A$, then $\bar{a}_1 + \bar{b}_1 \in A + B_1 \subset A + B$. If $\bar{a}_1 \in A'$, then $\bar{a}_1 = \bar{a}_o + \bar{b}$ where $\bar{b} \in B' \subset B$. Now $\bar{a}_o + \bar{b}_1 \in A$ for if not, then $\bar{b}_1 \in B'$ and we have a contradiction since $\bar{b}_1 \in B_1 = B \setminus B'$. Hence,

$$\bar{a}_1 + \bar{b}_1 = (\bar{a}_o + \bar{b}) + \bar{b}_1 = (\bar{a}_o + \bar{b}_1) + \bar{b} \in A + B.$$

Thus, $A_1 + B_1 \subset A + B$. This completes Case 2 and the theorem is proved.

CHAPTER III

SUMS OF SUBSETS OF N-DIMENSIONAL LATTICE POINTS: BASIS THEOREMS

Section 3-1. Introduction

We begin with some definitions.

Definition 3.1. Let $I = I^1$ denote the set of nonnegative integers and $I^n = \{(x_1, x_2, \ldots, x_n) \mid x_j \in I,\ j = 1, 2, \ldots, n\}$ for n a positive integer.

Definition 3.2.

1) For $x \in I^n$ and $x \neq 0 = (0, 0, \ldots, 0)$, let

$$L(x) = \{y \mid y \in I^n,\ y \neq 0,\ y_i \leq x_i,\ i = 1, 2, \ldots, n\},$$

2) $\mathcal{C} = \{L(x) \mid x \in I^n,\ x \neq 0\}$,

3) $\mathcal{K} = \{\cup_{x \in \Delta} L(x) \mid \Delta \subset I^n,\ 0 \notin \Delta,\ \Delta \text{ finite}\}$.

Definition 3.3. For $S, G \subset I^n$ and G finite, let $S(G)$ denote the number of nonzero elements in $S \cap G$.

Definition 3.4. The density α_C of Kasch of a set $A \subset I^n$ is given by $\alpha_C = \text{glb}\,\{A(H)/I^n(H) \mid H \in \mathcal{C}\}$.

Definition 3.5. The density α_K of Kvarda of a set $A \subset I^n$ is given by $\alpha_K = \text{glb}\,\{A(F)/I^n(F) \mid F \in \mathcal{K}\}$.

Definition 3.6. Let $A \subset I$ and let $A(n)$ denote the number of nonzero elements of A not exceeding n. The Schnirelmann density α of A is given by $\alpha = \text{glb}\{A(n)/n \mid n \in I,\ n \geq 1\}$.

We note that in I we have $\alpha_K = \alpha_C = \alpha$.

Definition 3.7. Let $A, B \subset I^n$. The sum $A + B$ of A and B is given by $A + B = A \cup B \cup \{a + b \mid a \in A,\ b \in B\}$.

Definition 3.8. Let $A_1, A_2, \ldots, A_h$, $h \geq 2$, be subsets of I^n. The sum of $A_1, A_2, \ldots, A_h$ is given recursively by

$$\sum_{i=1}^{h} A_i = A_h + \sum_{i=1}^{h-1} A_i.$$

Furthermore, if $A_i = A$, $i = 1, 2, \ldots, h$, $h \geq 1$, then $\Sigma_{i=1}^{h} A_i = hA$.

Definition 3.9. The set $A \subset I^n$ is a basis for I^n if there is a positive integer m such that $mA = I^n$. The order of A, denoted by $K = K(\alpha')$, is the least such positive integer. Here $\alpha' = \alpha_K$, $\alpha' = \alpha_C$, or $\alpha' = \alpha$.

The notation $K(\alpha')$ is used for the order of a basis set $A \subset I^n$ when an upper bound is given which is a function of α'. Actually the order K of A depends on much deeper properties of A than its density. In this chapter we obtain estimates for the order of a

basis set using the best density inequalities available for a sum. Then we compare these estimates.

The only theorems which are not original with the author are fundamental density inequality theorems which are clearly referenced. Little has been done before in obtaining or comparing order estimates for basis sets.

We conclude this section with some brief historical remarks. In 1930 L. Schnirelmann [23, 24] introduced his density to obtain results relating to Goldbach's conjecture. A flurry of activity followed for the space I culminating in Mann's Theorem of 1942. Some fundamental density inequalities for a sum in I are given in the following theorem.

Theorem 3.10. Let α, β and γ be the Schnirelmann densities of A, B and $A + B$ respectively. Then

1) If $\alpha = 1$, then $A = I$ (Schnirelmann [23], 1930);

2) If $\alpha + \beta \geq 1$, then $\gamma = 1$ (Schnirelmann [24], 1933);

3) $\gamma \geq \alpha + \beta - \alpha\beta$ (E. Landau [16] and Schnirelmann [24], 1933);

4) If $\alpha + \beta < 1$, then $\gamma \geq \beta/(1-\alpha)$ (I. Schur [25], 1936);

5) If $\alpha + \beta < 1$, then $\gamma \geq \alpha + \beta$ (H. Mann [17], 1942).

Several other authors have used modified densities in I including P. Erdös [8], A. Besicovitch [3], and R. Stalley [27]. Also several authors have extended density theory to I^n using densities

given by F. Kasch [14] and B. Kvarda [15] (Definitions 3.4 and 3.5). More general density theories have been developed by Freedman [9, 11] and others.

Section 3-2. Estimates of the Order of a Basis Set in I

We will use Theorem 3.10 Parts 1, 2 and 5 in this section.

Definition 3.11. Let $\gamma(h)$ be the Schnirelmann density of hA, and let α, β, and γ be the Schnirelmann densities of A, B and $A + B$ respectively.

Theorem 3.12. If $0 < \alpha < 1/2$, $h \geq 2$ and $\gamma(h-1) < 1 - \alpha$, then $\gamma(h) \geq h\alpha$.

Note that the statement of the theorem is vacuous without the condition $0 < \alpha < 1/2$.

Proof. We use Theorem 3.10 Part 5, namely if $\alpha + \beta < 1$ then $\gamma \geq \alpha + \beta$, and induction on h. For $h = 2$ we have $\gamma(2) \geq 2\alpha$ since $\gamma(1) = \alpha < 1 - \alpha$. Thus we assume the theorem holds for $h = k$ where $k \geq 2$ is fixed and assume $\gamma(k) < 1 - \alpha$. Since $\gamma(h)$ is a monotonically increasing function of h for $0 < \alpha < 1/2$ we have $\gamma(k-1) \leq \gamma(k) < 1 - \alpha$. Thus with sets A and B replaced by kA and B respectively we have

$$\gamma(k+1) \geq \gamma(k) + \alpha$$

$$\geq k\alpha + \alpha$$

$$= (k+1)\alpha .$$

Definition 3.13. Let x be real. The least integer not less than x is denoted $D(x)$. The greatest integer not greater than x, called the integer part of x, is denoted $E(x)$. The function F called the fractional part function is given by $F(x) = x - E(x)$.

Theorem 3.14. If $1/2 \leq \alpha \leq 1$, then A is a basis for I and has order $K(\alpha)$ equal to 1 if $\alpha = 1$ and equal to 2 if $1/2 \leq \alpha < 1$.

Proof. If $\alpha = 1$, then $A = I$ and by Definition 3.9 we have $K(\alpha) = 1$. If $1/2 \leq \alpha < 1$, then since $\alpha + \alpha \geq 1$, we have by Theorem 3.10 Part 2 that $\gamma(2) = 1$. Then by Theorem 3.10 Part 1 we have $2A = I$ and so $K(\alpha) = 2$.

Theorem 3.15. If $0 < \alpha < 1/2$, then A is a basis for I and has order

$$K(\alpha) \leq D(\frac{1}{\alpha}) .$$

Proof. The real number $h = \eta = (1-\alpha)/\alpha$ is the root of the equation

$$h\alpha = 1 - \alpha .$$

Hence let $h_o = D(\eta)$. Since $0 < \alpha < 1/2$, then $0 < \alpha < 1 - \alpha$. Then $\eta > 1$, and so $h_o \geq 2$. Hence if $\gamma(h_o - 1) < 1 - \alpha$, then by Theorem 3.12 we have

$$\gamma(h_o) \geq h_o \alpha$$

$$\geq \eta\alpha$$

$$= 1 - \alpha.$$

Since $\gamma(h_o) + \alpha \geq 1$, then by Theorem 3.10 Part 2 we have $\gamma(h_o + 1) = 1$. If $\gamma(h_o - 1) \geq 1 - \alpha$, then $\gamma(h_o - 1) + \alpha \geq 1$ and again by Theorem 3.10 Part 2 we have $\gamma(h_o) = 1$. Thus, in either case we have $\gamma(h_o + 1) = 1$. Finally, by Theorem 3.10 Part 1 we have

$$K(\alpha) \leq h_o + 1 = D(\frac{1-\alpha}{\alpha}) + 1 = D(\frac{1-\alpha}{\alpha} + 1) = D(\frac{1}{\alpha}).$$

Theorem 3.16. If $0 < \alpha < 1/2$ and $1/2 \leq s < 1 - \alpha$, then $\mathbf{A}$ is a basis for I and has order

$$K(\alpha) \leq D(\frac{s}{\alpha}) + D(\frac{1-s}{\alpha}).$$

Proof. Let the real number $h = \eta(s)$ be the root of the equation

$$h\alpha = 1 - s.$$

Then $\eta(s) = (1-s)/\alpha$ and $\eta(1-s) = s/\alpha$. Let $h_1 = D(\eta(1-s))$ and

$h_2 = D(\eta(s))$. Since $1/2 \leq s < 1 - \alpha$, then $\alpha < 1 - s \leq s$. Then $\eta(1-s) \geq \eta(s) > 1$, and so $h_1 \geq h_2 > 1$. Hence if $\gamma(h_1-1) < 1 - \alpha$, then $\gamma(h_2-1) < 1 - \alpha$. Then by Theorem 3.12 we have

$$\begin{aligned} \gamma(h_1) &\geq h_1\alpha \\ &\geq \eta(1-s)\alpha \\ &= s, \end{aligned}$$

and

$$\begin{aligned} \gamma(h_2) &\geq h_2\alpha \\ &\geq \eta(s)\alpha \\ &= 1 - s. \end{aligned}$$

Since $\gamma(h_1) + \gamma(h_2) \geq s + 1 - s = 1$, then by Theorem 3.10 Part 2 we have $\gamma(h_1+h_2) = 1$. If $\gamma(h_1-1) \geq 1 - \alpha$, then $\gamma(h_1-1) + \alpha \geq 1$ and again by Theorem 3.10 Part 2 we have $\gamma(h_1) = 1$. Thus, in either case we have $\gamma(h_1+h_2) = 1$. Finally, by Theorem 3.10 Part 1 we have

$$\begin{aligned} K(\alpha) &\leq h_1 + h_2 \\ &= D(\eta(1-s)) + D(\eta(s)) \\ &= D\left(\frac{s}{\alpha}\right) + D\left(\frac{1-s}{\alpha}\right). \end{aligned}$$

We note that values of s outside the interval $[1/2, 1-\alpha)$

would add nothing to this analysis.

The concluding theorem shows the bound for the order $K(\alpha)$ of A given by Theorem 3.15 is always as good as that given by Theorem 3.16.

Theorem 3.17. If $0 < \alpha < 1/2$ and $1/2 \leq s < 1 - \alpha$, then

$$D(\frac{1}{\alpha}) \leq D(\frac{s}{\alpha}) + D(\frac{1-s}{\alpha}) .$$

Proof. We have for real x and y by well known properties of the integer part function that

$$D(x) + D(y) = -E(-x) - E(-y) \geq -E(-(x+y)) = D(x+y).$$

Letting $x = s/\alpha$ and $y = (1-s)/\alpha$ we have

$$D(\frac{s}{\alpha}) + D(\frac{1-s}{\alpha}) \geq D(\frac{s}{\alpha} + \frac{1-s}{\alpha}) = D(\frac{1}{\alpha}).$$

Section 3-3. Estimates of the order of a Basis Set A in I^n Using α_C

In this section we obtain and compare estimates for the order of a basis set A with density α_C. We drop the density subscripts hereafter.

Definition 3.18. Let $\gamma(h)$ be the Kasch density of hA, and let α, β and γ be the Kasch densities of A, B and $A + B$

respectively.

Freedman [11] proved the following theorem.

Theorem 3.19 (Freedman). If $A, B \subset I^n$, then

1) If $\alpha = 1$, then $A = I^n$,

2) If $\alpha + \beta \geq 1$, then $\gamma = 1$,

3) $\gamma \geq \alpha + \beta\left(\frac{(1-\alpha)-(1-\alpha)^{n/(n-1)}}{n}\right)$.

We use this theorem to prove that if $\alpha > 0$, then A is a basis for I^n and to obtain some estimates for the order of A. In our first theorem we simply observe a limitation of Theorem 3.19 Part 3.

Theorem 3.20. If $\alpha < 1$ or $\beta < 1$, then $\gamma = 1$ does not follow from a single application of Theorem 3.19 Part 3.

Proof. We suppose

$$\alpha + \beta\left(\frac{(1-\alpha)-(1-\alpha)^{n/(n-1)}}{n}\right) \geq 1.$$

Then

$$\frac{\beta}{n}\left((1-\alpha)-(1-\alpha)^{n/(n-1)}\right) \geq 1 - \alpha,$$

from which it follows that

$$\frac{\beta}{n}\left(1-(1-\alpha)^{1/(n-1)}\right) \geq 1,$$

which is not satisfied by any α and β, $\alpha < 1$ and $\beta < 1$.

This result is not surprising; the same observation can be made about the inequality of Theorem 3.10 Part 3 in I.

The proof that if $\alpha > 0$, then A is a basis for I^n will involve repeated applications of Theorem 3.19 Part 3. In Theorem 3.34 we show that the most information about γ is obtained by substituting the larger density for α. Certain difficulties arise because the coefficient of β varies with α. We first examine this coefficient.

Definition 3.21. Let $f(\alpha) = \frac{(1-\alpha)-(1-\alpha)^{n/(n-1)}}{n}$.

Note the inequality of Theorem 3.19 Part 3 can be written $\gamma \geq \alpha + \beta f(\alpha)$.

Definition 3.22. Let $g(n) = 1 - (\frac{n-1}{n})^{n-1}$.

Theorem 3.23. If $0 < \alpha < 1$ and $n \geq 2$, then $f(\alpha)$ is

strictly increasing for $0 < \alpha \leq g(n)$ and strictly decreasing for $g(n) \leq \alpha < 1$.

Proof. First,

$$f'(\alpha) = \frac{1}{n}\left(-1+\frac{n}{n-1}(1-\alpha)^{1/(n-1)}\right).$$

Now $-1 + n(n-1)^{-1}(1-\alpha)^{1/(n-1)} = 0$ for $f(\alpha)$ to have a horizontal tangent. Solving this equation we obtain

$$(1-\alpha)^{1/(n-1)} = \frac{n-1}{n},$$

or

$$\alpha = 1 - \left(\frac{n-1}{n}\right)^{n-1} = g(n).$$

Next,

$$f''(\alpha) = \frac{1}{n}\left(\frac{n}{n-1}\right)\left(\frac{1}{n-1}\right)(1-\alpha)^{(2-n)/(n-1)}.$$

Since $1 - \alpha > 0$ for $0 < \alpha < 1$ we see that $f''(\alpha) < 0$ for $0 < \alpha < 1$ and $n \geq 2$ and the theorem follows.

Theorem 3.24. If x is a real variable, $x \geq 2$, then $g(x) = 1 - ((x-1)/x)^{x-1}$ is a strictly increasing function.

Proof.

$$g'(x) = -\left(\frac{x-1}{x}\right)^{x-1}\left[\log\frac{x-1}{x} + (x-1)\left(\frac{x}{x-1}\right)(x^{-2})\right]$$

$$= -\left(\frac{x-1}{x}\right)^{x-1}\left[\frac{1}{x} + \log(x-1) - \log x\right].$$

We show that $g'(x) > 0$ for $x \geq 2$. First we show that $x > (x-1)e^{1/x}$ for $x \geq 2$. Expanding $e^{1/x}$ and $x/(x-1)$ in power series of $1/x$ we see

$$e^{1/x} = \sum_{i=0}^{\infty} \frac{1}{i!} \left(\frac{1}{x}\right)^i$$

and

$$\frac{x}{x-1} = \frac{1}{1-1/x} = \sum_{i=0}^{\infty} \left(\frac{1}{x}\right)^i .$$

These power series are both convergent for $x \geq 2$, and so

$$\frac{x}{x-1} > e^{1/x} \quad \text{for} \quad x \geq 2.$$

Therefore

$$x > (x-1)e^{1/x} \quad \text{for} \quad x \geq 2.$$

However, then

$$\log x > \log (x-1) + \frac{1}{x},$$

or

$$\frac{1}{x} + \log (x-1) - \log x < 0.$$

Thus we see $g'(x) > 0$ and the theorem follows.

Theorem 3.25. If $n \geq 2$, then $g(n)$ is a strictly increasing function and $1/2 \leq g(n) < 1 - 1/e$.

Proof. That $g(n)$ is a strictly increasing function follows immediately from Theorem 3.24. For the second part we first note that $g(2) = 1 - 1/2 = 1/2$. Furthermore

$$\lim_{n\to\infty} g(n) = 1 - \lim_{n\to\infty} \left(\frac{n-1}{n}\right)^{n-1}$$

$$= 1 - \lim_{n\to\infty} \left(1-\frac{1}{n}\right)^{n-1}$$

$$= 1 - \frac{1}{e}.$$

Theorem 3.26. If $0 < \alpha < 1/2$ and $n \geq 2$, then $f(\alpha) \leq f(1-\alpha)$.

Proof. By Definition 3.21 we have

$$f(\alpha) = \frac{(1-\alpha)-(1-\alpha)^{n/(n-1)}}{n};$$

thus

$$f(1-\alpha) = \frac{\alpha-\alpha^{n/(n-1)}}{n}.$$

We observe $f(\alpha) = f(1-\alpha)$ for $n = 2$, so we assume $n \geq 3$. We let

$$y(\alpha) = n(f(1-\alpha)-f(\alpha))$$

$$= \alpha - \alpha^{n/(n-1)} - (1-\alpha) + (1-\alpha)^{n/(n-1)}$$

$$= 2\alpha - 1 - \alpha^{n/(n-1)} + (1-\alpha)^{n/(n-1)},$$

and show $y(\alpha) > 0$. Now

$$y'(\alpha) = 2 - \frac{n}{n-1}\left(\alpha^{1/(n-1)} + (1-\alpha)^{1/(n-1)}\right),$$

and so

$$y''(\alpha) = -\frac{n}{(n-1)^2}\left(\alpha^{\frac{2-n}{n-1}} - (1-\alpha)^{\frac{2-n}{1-n}}\right).$$

However since $0 < \alpha < 1/2$, then $\alpha < 1 - \alpha$, or $1/\alpha > 1/(1-\alpha)$. Consequently

$$\alpha^{\frac{2-n}{n-1}} = \left(\frac{1}{\alpha}\right)^{\frac{n-2}{n-1}} > \left(\frac{1}{1-\alpha}\right)^{\frac{n-2}{n-1}} = (1-\alpha)^{\frac{2-n}{n-1}}$$

for $n \geq 3$. Thus we see that $y''(\alpha) < 0$. Since $y(0) = y(1/2) = 0$ and $y(\alpha)$ has downward concavity, we conclude $y(\alpha) > 0$ for $0 < \alpha < 1/2$ and $n \geq 3$.

Theorem 3.27. Let α, n be fixed, $0 < \alpha < 1/2$, $n \geq 2$, and let γ be real. If $\alpha \leq \gamma \leq 1 - \alpha$, then $f(\alpha) \leq f(\gamma)$.

Proof. If $\alpha \leq \gamma \leq g(n)$, then by Theorem 3.23 we have $f(\alpha) \leq f(\gamma)$. Thus we assume $g(n) < \gamma \leq 1 - \alpha$. It follows from Theorem 3.25 that $\gamma > 1/2$, and so $0 < 1 - \gamma < 1/2$. By Theorem 3.26 we have $f(1-\gamma) \leq f(\gamma)$. Since $\gamma \leq 1 - \alpha$, then by Theorem 3.25 we have $\alpha \leq 1 - \gamma < g(n)$, and so by Theorem 3.23 we have $f(\alpha) \leq f(1-\gamma) \leq f(\gamma)$. This completes the proof.

This concludes the examination of $f(\alpha)$ and we now proceed to establish the basis theorems.

Theorem 3.28. If $0 < \alpha < 1/2$, $n \geq 2$, $h \geq 2$ and $\gamma(h-1) < 1 - \alpha$, then $\gamma(h) \geq \alpha + (h-1)\alpha f(\alpha)$.

Proof. We use induction on h. If $h = 2$, then note that $\gamma(h-1) = \alpha < 1 - \alpha$. Theorem 3.19 Part 3 states that

$$\gamma \geq \alpha + \beta f(\alpha) .$$

For $B = A$ we see

$$\gamma(2) \geq \alpha + \alpha f(\alpha),$$

thus the theorem follows for $h = 2$.

Thus we assume the theorem holds for $h = k$ where $k \geq 2$ is fixed and assume $\gamma(k) < 1 - \alpha$. Since $\gamma(h)$ is a monotonically increasing function of h for $0 < \alpha < 1/2$, we have by Theorem 3.19 Part 3 that

$$\alpha < \gamma(2) \leq \gamma(k) < 1 - \alpha .$$

Thus, by Theorem 3.27 we have

$$f(\alpha) \leq f(\gamma(k)).$$

Also, since $\gamma(k-1) \leq \gamma(k) < 1 - \alpha$, the conclusion of the theorem

holds with k replaced by $k - 1$. Therefore, with sets A and B replaced by kA and A respectively in Theorem 3.19 Part 3 we have

$$\begin{aligned}\gamma(k+1) &\geq \gamma(k) + \alpha f(\gamma(k)) \\ &\geq \gamma(k) + \alpha f(\alpha) \\ &\geq \alpha + (k-1)\alpha f(\alpha) + \alpha f(\alpha) \\ &= \alpha + (k)\alpha f(\alpha).\end{aligned}$$

We now show if $\alpha > 0$, then A is a basis for I^n and obtain two estimates for the order of A.

Theorem 3.29. If $1/2 \leq \alpha < 1$, then A is a basis for I^n and has order $K(\alpha)$ equal to 1 if $\alpha = 1$ and equal to 2 if $1/2 \leq \alpha < 1$.

Proof. See Theorem 3.14.

Theorem 3.30. If $0 < \alpha < 1/2$ and $n \geq 2$, then A is a basis for I^n and has order

$$K(\alpha) \leq D(\zeta) + 2$$

where

$$\zeta = \frac{1-2\alpha}{\alpha f(\alpha)}.$$

Proof. The real number $h = \rho = \zeta + 1$ is the root of the

equation

$$\alpha + (h-1)\alpha f(\alpha) = 1 - \alpha .$$

Hence let $h_o = D(\rho)$. Then $h_o \geq 2$ since $\rho > 1$. Hence if $\gamma(h_o-1) < 1 - \alpha$, then by Theorem 3.28 we have

$$\begin{aligned} \gamma(h_o) &\geq \alpha + (h_o-1)\alpha f(\alpha) \\ &\geq \alpha + (\rho-1)\alpha f(\alpha) \\ &= 1 - \alpha . \end{aligned}$$

Since $\gamma(h_o) + \alpha \geq 1$, then by Theorem 3.19 Parts 1 and 2 $\gamma(h_o+1) = 1$. If $\gamma(h_o-1) \geq 1 - \alpha$, then $\gamma(h_o-1) + \alpha \geq 1$, and so $\gamma(h_o) = 1$. Thus in either case $\gamma(h_o+1) = 1$. Finally

$$\begin{aligned} K(\alpha) &\leq h_o + 1 = D(\rho) + 1 \\ &= D(\zeta+1)^{+1} = D(\zeta) + 2. \end{aligned}$$

Theorem 3.31. If $0 < \alpha < 1/2$ and $n \geq 2$, then A is a basis for I^n and has order

$$K(\alpha) \leq D(\zeta_1) + 2$$

where

$$\zeta_1 = \frac{n(n-1)(1-2\alpha)}{\alpha^2(1-\alpha)} .$$

Proof. By Theorem 3.30 we have

$$\zeta = \frac{1-2a}{af(a)} = \frac{(1-2a)n}{a((1-a)-(1-a)^{n/(n-1)})} = \frac{(1-2a)n}{a(1-a)(1-(1-a)^{1/(n-1)})} .$$

Now

$$(1-a)^{1/(n-1)} = 1 - \frac{1}{n-1}\,a + \frac{(\frac{1}{n-1})(\frac{1}{n-1}-1)a^2}{2!} + \ldots$$

$$< 1 - \frac{1}{n-1}\,a ,$$

since all the terms in the binomial expansion after the first term are negative. Hence

$$\zeta = \frac{(1-2a)}{a(1-a)(1-(1-a)^{1/(n-1)})}$$

$$< \frac{(1-2a)n}{a(1-a)((n-1)^{-1}a)}$$

$$= \frac{n(n-1)(1-2a)}{a^2(1-a)} .$$

Theorem 3.32. Let $n \geq 2$. If $0 < a < 1/2$ and $1/2 \leq s < 1 - a$, then A is a basis for I^n and has order

$$K(a) \leq D(\eta(1-s)) + D(\eta(s))$$

where

$$\eta(s) = \frac{1-s-a}{af(a)} + 1 .$$

Proof. Let the real number $h = \eta(s)$ be the root of the

equation

$$\alpha + (h-1)\alpha f(\alpha) = 1 - s.$$

Then

$$\eta(s) = \frac{1-s-\alpha}{\alpha f(\alpha)} + 1$$

and

$$\eta(1-s) = \frac{s-\alpha}{\alpha f(\alpha)} + 1.$$

Let $h_1 = D(\eta(1-s))$ and $h_2 = D(\eta(s))$. Since $1/2 \leq s < 1 - \alpha$, then $\alpha < 1 - s \leq s$, and so $0 < 1 - s - \alpha \leq s - \alpha$. Thus $\eta(1-s) \geq \eta(s) > 1$, and so $h_1 \geq h_2 \geq 2$. Hence if $\gamma(h_1-1) < 1 - \alpha$, then $\gamma(h_2-1) < 1 - \alpha$. Then by Theorem 3.28 we have

$$\begin{aligned}\gamma(h_1) &\geq \alpha + (h_1-1)\alpha f(\alpha) \\ &\geq \alpha + (\eta(1-s)-1)\alpha f(\alpha) \\ &= s,\end{aligned}$$

and

$$\begin{aligned}\gamma(h_2) &\geq \alpha + (h_2-1)\alpha f(\alpha) \\ &\geq \alpha + (\eta(s)-1)\alpha f(\alpha) \\ &= 1 - s.\end{aligned}$$

Since $\gamma(h_1) + \gamma(h_2) \geq s + 1 - s = 1$, then by Theorem 3.19 Part 2 we have $\gamma(h_1+h_2) = 1$. If $\gamma(h_1-1) \geq 1 - \alpha$, then $\gamma(h_1-1) + \alpha \geq 1$ and again by Theorem 3.19 Part 2 we have $\gamma(h_1) = 1$. Thus, in

either case we have $\gamma(h_1+h_2) = 1$. Finally, by Theorem 3.19 Part 1 we have

$$K(\alpha) \leq h_1 + h_2$$

$$= D(\eta(1-s)) + D(\eta(s)).$$

The theorem follows.

The following theorem shows the bound for the order $K(\alpha)$ of A given by Theorem 3.30 is always as good as that given by Theorem 3.32.

Theorem 3.33. Let $n \geq 2$, $0 < \alpha < 1/2$, $1/2 \leq s < 1 - \alpha$. If $\zeta = (1-2\alpha)/\alpha f(\alpha)$, and $\eta(s) = (1-s-\alpha)/\alpha f(\alpha) + 1$, then

$$D(\eta(s)) + D(\eta(1-s)) \geq D(\zeta) + 2.$$

Proof.

$$D(\eta(s)) + D(\eta(1-s)) \geq D(\eta(s)+\eta(1-s))$$

$$= D\left(\frac{1-s-\alpha}{\alpha f(\alpha)} + 1 + \frac{s-\alpha}{\alpha f(\alpha)} + 1\right)$$

$$= D\left(\frac{1-2\alpha}{\alpha f(\alpha)}\right) + 2$$

$$= D(\zeta) + 2.$$

We complete the study of estimating the order of a basis set A using Theorem 3.19 Part 3 by showing the substitution employed in Theorem 3.28 gives the most information about $\gamma(h)$.

Theorem 3.34. If $0 < \alpha < \gamma < 1$ and $n \geq 2$ then

$$\gamma + \alpha f(\gamma) > \alpha + \gamma f(\alpha).$$

Proof. By hypothesis $0 < \alpha < \gamma < 1$, and so

$$1 - \alpha > 1 - \gamma > 0.$$

Hence

$$(1-\alpha)^{n/(n-1)} > (1-\gamma)^{n/(n-1)} > 0,$$

and so

(1) $$\gamma(1-\alpha)^{n/(n-1)} > \alpha(1-\gamma)^{n/(n-1)}.$$

Also $(n-1)\gamma > (n-1)\alpha$, and so

(2) $$n\gamma - \gamma(1-\alpha) > n\alpha - \alpha(1-\gamma).$$

Adding inequalities (1) and (2) we obtain

$$n\gamma - \gamma[(1-\alpha)-(1-\alpha)^{n/(n-1)}] > n\alpha - \alpha[(1-\gamma)-(1-\gamma)^{n/(n-1)}],$$

which is

$$n\gamma - \gamma n f(\alpha) > n\alpha - \alpha n f(\gamma)$$

and the theorem follows.

Kasch [14] suggests a different procedure to show that if $\alpha > 0$, then A is a basis for I^n. We use this procedure to prove the next theorem.

Definition 3.35. Let

1) $x^i = (x_1, x_2, \ldots, x_n) \in I^n$ where $x_j = 0$ if $j \neq i$;

2) $X_i = \{x^i \mid x^i \in I^n\}$

3) $\alpha_i = \text{glb } \{A(L(x^i))/I^n(L(x^i)) \mid L(x^i) \in \mathfrak{C}\}$.

Theorem 3.36. If h_i is a bound for the order of $A \cap X_i$, $i = 1, 2, \ldots, n$, then A is a basis for I^n and has order

$$K \leq \sum_{i=1}^{n} h_i.$$

Proof. Since $h_i(A \cap X_i) = X_i$ for $i = 1, 2, \ldots, n$, then

$$\sum_{i=1}^{n} h_i(A \cap X_i) = \sum_{i=1}^{n} X_i .$$

If $y \in I^n$, then $y \in \Sigma_{i=1}^{n} X_i$. Also $h_i(A \cap X_i) \subset h_i A$ for $i = 1, 2, \ldots, n$. Hence

$$I^n = \sum_{i=1}^{n} X_i = \sum_{i=1}^{n} h_i(A \cap X_i) \subset \sum_{i=1}^{n} (h_i A)$$

$$= \left(\sum_{i=1}^{n} h_i \right) A \subset I^n,$$

and so $(\Sigma_{i=1}^{n} h_i)A = I^n$. The theorem follows.

This theorem can be used to obtain a bound for the order of a basis set A. We first prove a lemma.

Lemma 3.37. We have $\alpha \leq \alpha_i$ for $i = 1, 2, \ldots, n$.

Proof. We note that $L(x^i) \in \mathcal{C}$, and thus

$$\left\{ \frac{A(L(x^i))}{I^n(L(x^i))} \;\middle|\; L(x^i) \in \mathcal{C} \right\} \subset \left\{ \frac{A(L(x))}{I^n(L(x))} \;\middle|\; L(x) \in \mathcal{C} \right\}.$$

Taking the greatest lower bound of each set gives the lemma.

Theorem 3.38. If $0 < \alpha < 1/2$, $n \geq 1$, then A is a basis for I^n and has order

$$K(\alpha) \leq nD(\frac{1}{\alpha}).$$

Proof. It follows from Lemma 3.37 that $\alpha \leq \alpha_i$, $i = 1,2,\ldots,n$. Since each X_i is a copy of I, we have by Theorem 3.15 that

$h_i \leq D(1/\alpha_i)$ where h_i is defined in the statement of Theorem 3.36. Then by Theorem 3.36 we see that

$$K(\alpha) = K \leq \sum_{i=1}^{n} h_i \leq \sum_{i=1}^{n} D(\frac{1}{\alpha_i})$$

$$\leq \sum_{i=1}^{n} D(\frac{1}{\alpha}) = nD(\frac{1}{\alpha}).$$

We conclude this section with a comparison of the bound for the order of a basis set A given in Theorem 3.31 with that given in Theorem 3.38.

Theorem 3.39. If $n \geq 2$ and $0 < \alpha < 1/3$, then $nD(1/\alpha) < D(\zeta_1) + 2$ where

$$\zeta_1 = \frac{n(n-1)(1-2\alpha)}{\alpha^2(1-\alpha)}.$$

Note that we actually prove that $nD(1/\alpha) \leq D(\zeta_1) - 1$.

Proof of Theorem 3.39. Let $1/q \leq \alpha < 1/(q-1)$ where q is a positive integer, $q \geq 4$. Then

(1)
$$\zeta_1 = \frac{n(n-1)(1-2a)}{a^2(1-a)}$$
$$> \frac{n(n-1)(1-2/(q-1))}{(1/(q-1))^2(1-1/q)}$$
$$= n(n-1)q(q-3).$$

Now $q \geq 1/a > q-1$, and since $D(x)$ is integer valued we have $q \geq D(1/a) > q-1$, or finally $D(1/a) = q$. Hence since $n \geq 2$ and $q \geq 4$ we have by inequality (1) that

$$\zeta_1 > nq = nD(\frac{1}{a}).$$

Hence $D(\zeta_1) - 1 \geq nD(1/a)$, and the theorem follows.

Lemma 3.40. Let $y(a) = a^3 - a^2 - 2ca + c$ where $c \geq 1/2$. Then

$$\frac{1}{2}\frac{72c+2}{72c+11} > \frac{1}{3},$$

and if

$$\frac{1}{2}\frac{72c+2}{72c+11} \leq a < \frac{1}{2},$$

then $y(a) \leq 0$.

Proof. Since $c \geq 1/2$, then

$$\frac{1}{2}\frac{72c+2}{72c+11} \geq \frac{1}{2}\frac{36+2}{36+11} = \frac{19}{47} > \frac{1}{3}.$$

Now $y'(a) = 3a^2 - 2a - 2c$ and, for $c \geq 1/2$ and $1/3 < a < 1/2$, we have $y'(a) < 3(1/2)^2 - 2(1/3) - 2(1/2) = -11/12 < 0$. Thus $y(a)$ is decreasing for $1/3 < a < 1/2$. Furthermore

$y(1/3) = c/3 - 2/27 \geq 1/6 - 2/27 = 5/54 > 0$ and $y(1/2) = -1/8 < 0$.

Hence $y(a) = 0$ for exactly one value of a where $1/3 < a < 1/2$. Let $y = L(a)$ be the secant line containing the points $(1/3, c/3 - 2/27)$ and $(1/2, -1/8)$ of $y = y(a)$. Since $y''(a) = 6a - 2 > 0$ for $a > 1/3$, then $y = y(a)$ is concave upward and so $y(a) \leq L(a)$ for $1/3 < a < 1/2$.

The equation for line L is

$$y + \frac{1}{8} = \frac{c/3 - 2/27 + 1/8}{1/3 - 1/2}\left(a - \frac{1}{2}\right)$$

$$= -\frac{72c+11}{36}\left(a - \frac{1}{2}\right).$$

Hence the a intercept of L is

$$a = -\frac{9}{2}\frac{1}{72c+11} + \frac{1}{2}$$

$$= \frac{1}{2}\frac{72c+2}{72c+11}.$$

Finally, if $(1/2)(72c+2)/(72c+11) \leq a < 1/2$, then $L(a) \leq 0$, and since $(1/2)(72c+2)/(72c+11) > 1/3$, then $y(a) \leq 0$.

Theorem 3.41. If $n \geq 2$,

$$\zeta_1 = \frac{n(n-1)(1-2a)}{a^2(1-a)},$$

and

$$\frac{1}{2}\frac{72n^2-66n-4}{72n^2-39n-22} \leq a < \frac{1}{2},$$

then $D(\zeta_1) + 2 \leq nD(1/a)$.

Proof. Let $c = n(n-1)/(3n-2)$. Then $c \geq 1/2$ since $n \geq 2$. Since

$$\frac{1}{2}\frac{72c+2}{72c+11} = \frac{1}{2}\frac{72n(n-1)+2(3n-2)}{72n(n-1)+11(3n-2)}$$

$$= \frac{1}{2}\frac{72n^2-66n-4}{72n^2-39n-22},$$

then $a \geq (1/2)(72c+2)/(72c+11)$. Since $a < 1/2$, then by Lemma 3.40 we have $y(a) \leq 0$ where

$$y(a) = a^3 - a^2 - 2ca + c$$

$$= a^3 - a^2 - \frac{2n(n-1)}{3n-2}a + \frac{n(n-1)}{3n-2}.$$

Hence

$$(3n-2)a^3 - (3n-2)a^2 - 2n(n-1)a + n(n-1) \leq 0,$$

or

$$n(n-1)(1-2a) + 2a^2 - 2a^3 \leq 3na^2 - 3na^3,$$

from which it follows that

$$\frac{n(n-1)(1-2a)}{a^2(1-a)} + 2 \leq 3n.$$

We have by Lemma 3.40 that $1/3 < a < 1/2$, and so $2 < 1/a < 3$, from which it follows that

$$D(\zeta_1) + 2 = D(\zeta_1 + 2) \leq D(3n)$$

$$= 3n = nD(\frac{1}{a}) .$$

We consider an example. Let $n = 3$. Then

$$a \geq \frac{1}{2} \frac{72n^2 - 66n - 4}{72n^2 - 39n - 22} = \frac{223}{509} .$$

Let $a = 5/11$. Then

$$\zeta_1 = \frac{n(n-1)(1-2a)}{a^2(1-a)} = \frac{121}{25} .$$

Hence $D(\zeta_1) + 2 = 7$ while $nD(1/a) = 9$.

We note that Theorems 3.39 and 3.41 give no comparison of the estimates of the order of A for a in the interval

$$\frac{1}{3} \leq a < f(n) = \frac{1}{2} \frac{72n^2 - 66n - 4}{72n^2 - 39n - 22} ,$$

where $n \geq 2$. For $n \geq 2$ the function $f(n)$ is increasing and $f(n) \geq 19/47$. Also $\lim_{n \to \infty} f(n) = 1/2$. In particular, $f(2) = 19/47$,

$f(3) = 233/509$ and $f(4) = 221/487$. The author has been unsuccessful in decreasing the length of this interval. There are several approaches. One approach is to reduce the round off error of the binomial expansion approximation in Theorem 3.31. A second approach is to replace the secant line of Theorem 3.41 with a better fitting curve. A third approach is to replace $f(\gamma)$ in the proof of Theorem 3.28 by something larger than $f(\alpha)$ to obtain a different expression.

Section 3-4. Estimates of the Order of a Basis Set A In I^n Using α_K

In this section we obtain and compare estimates for the order of a basis set A with density α_K. We drop the density subscripts hereafter.

Definition 3.42. Let $\gamma(h)$ be the Kvarda density of hA, and let α, β, and γ be the Kvarda densities of A, B and $A + B$ respectively.

Theorem 3.43. The following density theorems hold in I^n.

1) If $\alpha = 1$, then $A = I^n$ Kvarda [15];

2) If $\alpha + \beta \geq 1$, then $\gamma = 1$ Kvarda [15];

3) $\gamma \geq \alpha + \beta - \alpha\beta$ Kvarda [15];

4) If $\alpha + \beta < 1$, then $\gamma \geq \beta/(1-\alpha)$ Freedman [11].

Theorem 3.44. If $1/2 \leq \alpha \leq 1$, then A is a basis for I^n and has order $K(\alpha)$ equal to 1 if $\alpha = 1$ and equal to 2 if $1/2 \leq \alpha < 1$.

Proof. See Theorem 3.14.

Kvarda [15] proved the following theorem. We give a modification of her proof.

Theorem 3.45. It follows from the density inequality $\gamma \geq \alpha + \beta - \alpha\beta$, that $\gamma(h) \geq 1 - (1-\alpha)^h$ for $h \geq 1$.

Proof. We use induction on h. For $h = 1$ we have $\gamma(1) = \gamma = \alpha = 1 - (1-\alpha)$. Thus we assume the theorem holds for $h = k$ where $k \geq 1$ is fixed. In $\gamma \geq \alpha + \beta - \alpha\beta$ with sets A and B replaced by kA and B respectively we have

$$\begin{aligned}
\gamma(k+1) &\geq \alpha + \gamma(k) - \alpha\gamma(k) \\
&= \alpha + \gamma(k)\ (1-\alpha) \\
&\geq \alpha + (1-(1-\alpha)^k)(1-\alpha) \\
&= 1 - (1-\alpha)^{k+1}.
\end{aligned}$$

Theorem 3.46. If $0 < \alpha < 1/2$ and $1/2 \leq s \leq 1 - \alpha$, then A is a basis for I^n and has order

$$K(\alpha) = D\left(\frac{\log s}{\log (1-\alpha)}\right) + D\left(\frac{\log (1-s)}{\log (1-\alpha)}\right) .$$

Proof. Let the real number $h = \eta(s)$ be the root of the equation

$$1 - (1-\alpha)^{h} = 1 - s.$$

Then $\eta(s) = (\log s)/\log (1-\alpha)$ and $\eta(1-s) = \log (1-s)/\log (1-\alpha)$. Let $h_1 = D(\eta(1-s))$ and $h_2 = D(\eta(s))$. By Theorem 3.45 we have

$$\begin{aligned} \gamma(h_1) &\geq 1 - (1-\alpha)^{h_1} \\ &\geq 1 - (1-\alpha)^{\eta(1-s)} \\ &= s, \end{aligned}$$

and

$$\begin{aligned} \gamma(h_2) &\geq 1 - (1-\alpha)^{h_2} \\ &\geq 1 - (1-\alpha)^{\eta(s)} \\ &= 1 - s. \end{aligned}$$

Since $\gamma(h_1) + \gamma(h_2) \geq s + 1 - s = 1$, then by Theorem 3.43 Part 2 we have $\gamma(h_1+h_2) = 1$. Hence by Theorem 3.43 Part 1 we have

$$\begin{aligned} K(\alpha) &\leq h_1 + h_2 \\ &= D(\eta(1-s)) + D(\eta(s)) \\ &= D\left(\frac{\log (1-s)}{\log (1-\alpha)}\right) + D\left(\frac{\log s}{\log (1-\alpha)}\right) . \end{aligned}$$

This completes the proof.

Theorem 3.47. If $0 < a < 1/2$, then A is a basis for I^n and has order $K(a)$ where

$$K(a) \leq D(\frac{\log a}{\log (1-a)}) + 1$$

and

$$K(a) \leq 2D(\frac{-\log 2}{\log (1-a)}) .$$

Proof. Letting $s = 1 - a$ and $s = 1/2$ in Theorem 3.46 gives the first and second bounds respectively.

If we attempt to analyze the bound over the interval $1/2 \leq s \leq 1 - a$ as was done in Theorems 3.17 and 3.33 we obtain

$$(1) \qquad D(\frac{\log s}{\log (1-a)}) + D(\frac{\log (1-s)}{\log (1-a)}) \geq D(\frac{\log s(1-s)}{\log (1-a)}) .$$

If $1/2 \leq s \leq 1 - a$, then $s(1-s)$ is maximum for $s = 1/2$ and minimum for $s = 1 - a$. Since $0 < a < 1/2$, then $\log (1-a)$ is negative, and so $(\log s(1-s))/\log (1-a)$ is maximum at $s = 1 - a$ and minimum at $s = 1/2$. Thus setting $s = 1 - a$ in inequality (1) we obtain

$$D\left(\frac{\log(1-\alpha)}{\log(1-\alpha)}\right) + D\left(\frac{\log \alpha}{\log(1-\alpha)}\right) = D\left(\frac{\log \alpha}{\log(1-\alpha)}\right) + 1 \geq D\left(\frac{\log \alpha(1-\alpha)}{\log(1-\alpha)}\right)$$

$$\geq D\left(\frac{-2\log 2}{\log(1-\alpha)}\right).$$

However setting $s = 1/2$ in the left member of inequality (1) we obtain

$$D\left(\frac{-\log 2}{\log(1-\alpha)}\right) + D\left(\frac{-\log 2}{\log(1-\alpha)}\right) = 2D\left(\frac{-\log 2}{\log(1-\alpha)}\right) \geq D\left(\frac{-2\log 2}{\log(1-\alpha)}\right).$$

Since the right hand expressions are the same we see that the inequality reverses and no comparison can be made by this method. In fact the bounds for $K(\alpha)$ obtained in Theorem 3.47 are incomparable as we show in Theorem 3.53.

Theorem 3.48. It follows from the density theorem, if $\alpha + \beta < 1$, then $\gamma \geq \beta/(1-\alpha)$, that if $\gamma(h-1) < 1 - \alpha$ and $h \geq 2$, then $\gamma(h) \geq \alpha/(1-\alpha)^{h-1}$.

Proof. We use induction on h. For $h = 2$ we have $\gamma(2) = \alpha/(1-\alpha)$ since $\gamma(1) = \alpha < 1 - \alpha$. Thus we assume the theorem holds for $h = k$ where $k \geq 2$ is fixed and assume $\gamma(k) < 1 - \alpha$. Since $\gamma(h)$ is a monotonically increasing function of h for $0 < \alpha < 1/2$ we have $\gamma(k-1) \leq \gamma(k) < 1 - \alpha$. Thus with sets A and B replaced with A and kA respectively we have

$$\gamma(k+1) \geq \frac{\gamma(k)}{1-\alpha}$$

$$> \frac{\alpha/(1-\alpha)^{k-1}}{1-\alpha}$$

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

Theorem 3.49. If $0 < \alpha < 1/2$, then A is a basis for I^n and has order

$$K(\alpha) \leq D(\zeta) + 1$$

where

$$\zeta = \frac{\log \alpha}{\log (1-\alpha)} .$$

Proof. The real number $h = \zeta$ is the root of the equation

$$\frac{\alpha}{(1-\alpha)^{n-1}} = 1 - \alpha .$$

Hence let $h_o = D(\zeta)$. Since $0 < \alpha < 1/2$, then $0 < \alpha < 1 - \alpha$. Thus $\zeta > 1$, and so $h_o \geq 2$. If $\gamma(h_o - 1) < 1 - \alpha$, then by Theorem 3.48 we have

$$\gamma(h_o) \geq \frac{\alpha}{(1-\alpha)^{h_o-1}}$$

$$\geq \frac{\alpha}{(1-\alpha)^{\zeta-1}}$$

$$= 1 - \alpha .$$

Since $\gamma(h_o) + \alpha \geq 1$, then by Theorem 3.43 Part 2 we have $\gamma(h_o+1) = 1$. If $\gamma(h_o-1) \geq 1 - \alpha$, then again by Theorem 3.43 Part 2 we have $\gamma(h_o) = 1$. Thus in either case we have $\gamma(h_o+1) = 1$. Finally by Theorem 3.43 Part 1 we have

$$K(\alpha) \leq h_o + 1 = D(\zeta) + 1.$$

Theorem 3.50. If $0 < \alpha < 1/2$ and $1/2 \leq s < 1 - \alpha$, then A is a basis for I^n and has order

$$K(\alpha) \leq D(\eta(1-s)) + D(\eta(s))$$

where

$$\eta(s) = \frac{\log \alpha - \log (1-s)}{\log (1-\alpha)} + 1$$

Proof. Let the real number $h = \eta(s)$ be the root of the equation

$$\frac{\alpha}{(1-\alpha)^{h-1}} = 1 - s.$$

Then

$$\eta(s) = \frac{\log \alpha - \log (1-s)}{\log (1-\alpha)} + 1,$$

and

$$\eta(1-s) = \frac{\log \alpha - \log s}{\log (1-\alpha)} + 1.$$

Let $h_1 = D(\eta(1-s))$ and $h_2 = D(\eta(s))$. Since $1/2 \leq s < 1 - \alpha$,

then $\alpha < 1 - s \leq s$. Thus $\eta(1-s) \geq \eta(s) > 1$, and so $h_1 \geq h_2 \geq 2$. Hence if $\gamma(h_1-1) < 1 - \alpha$, then $\gamma(h_2-1) < 1 - \alpha$. Then by Theorem 3.48 we have

$$\gamma(h_1) \geq \frac{\alpha}{(1-\alpha)^{h_1-1}}$$

$$\geq \frac{\alpha}{(1-\alpha)^{\eta(1-s)-1}}$$

$$= s,$$

and

$$\gamma(h_2) \geq \frac{\alpha}{(1-\alpha)^{h_2-1}}$$

$$\geq \frac{\alpha}{(1-\alpha)^{\eta(s)-1}}$$

$$= 1 - s.$$

Since $\gamma(h_1) + \gamma(h_2) \geq s + 1 - s = 1$, then by Theorem 3.43 Part 2 we have $\gamma(h_1+h_2) = 1$. If $\gamma(h_1-1) \geq 1 - \alpha$, then $\gamma(h_1-1) + \alpha \geq 1$ and again by Theorem 3.43 Part 2 we have $\gamma(h_1) = 1$. Thus by Theorem 3.43 Part 1 we have

$$K(\alpha) \leq h_1+h_2$$

$$= D(\eta(1-s)) + D(\eta(s)).$$

This completes the proof.

As with Theorem 3.46 an analysis similar to Theorems 3.17 and 3.33 is not possible. We obtain a second bound for $K(\alpha)$ at the end point $s = 1/2$.

Theorem 3.51. If $0 < a < 1/2$, then A is a basis for I^n and has order

$$K(a) = 2D(\eta) + 2$$

where

$$\eta = \frac{\log 2a}{\log (1-a)} .$$

Proof. Letting $s = 1/2$ in Theorem 3.50 proves the theorem.

Lemma 3.52. Let x be real. Then $D(2x) = 2D(x)$ if $F(x) = 0$ or if $F(x) \geq 1/2$. Also $D(2x) = 2D(x) - 1$ if $0 < F(x) < 1/2$.

Proof. If $F(x) = 0$ the theorem is immediate. Hence we assume $F(x) > 0$ from which it follows that $2D(x) = 2E(x) + 2$. Since $x = E(x) + F(x)$, then $D(2x) = 2E(x) + D(2F(x))$. Hence if $F(x) \geq 1/2$, then $1 \leq 2F(x) < 2$, and so $D(2x) = 2E(x) + 2 = 2D(x)$. Finally if $0 < F(x) < 1/2$, then $0 < 2F(x) < 1$, and so $D(2x) = 2E(x) + 1 = 2D(x) - 1$.

The following theorem compares the bounds for the order $K(a)$ of A given by Theorem 3.47, Theorem 3.49 and Theorem 3.51. The bounds of Theorem 3.47 are incomparable. However one of these is always as good as the bounds of Theorems 3.49 and 3.51.

Theorem 3.53. Let $0 < a < 1/2$, $\zeta = (\log a)/\log (1-a)$, $\xi = -(\log 2)/\log (1-a)$, and $\eta = (\log 2a)/\log (1-a)$. Then $D(\zeta) + 1 \leq 2D(\eta) + 2$. If $F(\xi) \geq 1/2$ or $F(\xi) = 0$, then $2D(\xi) \leq D(\zeta) + 1$. If $F(\xi) < 1/2$ and $a \leq 1/4$, then again

$2D(\xi) \leq D(\zeta) + 1$. Finally if $0 < F(\xi) < 1/2$ and $\alpha > 1/4$, then $D(\zeta) + 1 \leq 2D(\xi)$.

Proof. Since $4\alpha^2 - 4\alpha + 1 = (2\alpha-1)^2 \geq 0$, then

$$1 \geq 4\alpha - 4\alpha^2, \tag{1}$$

and so $\alpha \geq 4\alpha^2(1-\alpha)$. Hence $\log \alpha \geq 2 \log 2\alpha + \log (1-\alpha)$, and since $0 < \alpha < 1/2$, then $(\log \alpha)/\log (1-\alpha) \leq 2(\log \alpha)/\log (1-\alpha) + 1$, or $\zeta \leq 2\eta + 1$. Thus $D(\zeta) + 1 \leq D(2\eta+1) + 1 = D(2\eta) + 2 \leq 2D(\eta) + 2$.

Next assume $F(\xi) \geq 1/2$ or $F(\xi) = 0$. Then $D(2\xi) = 2D(\xi)$. From the inequality (1) we have $1/4 \geq \alpha(1-\alpha)$, and so $-2 \log 2 \geq \log \alpha + \log (1-\alpha)$. Hence since $0 < \alpha < 1/2$, then $-2 (\log 2)/\log (1-\alpha) \leq (\log \alpha)/\log (1-\alpha) + 1$, or $2\xi \leq \zeta + 1$. Thus $2D(\xi) = D(2\xi) \leq D(\zeta+1) = D(\zeta) + 1$.

Next assume $0 < F(\xi) < 1/2$ and $\alpha \leq 1/4$. Then $D(2\xi) = 2D(\xi) - 1$. Since $\alpha \leq 1/4$, then $\log \alpha \leq -2 \log 2$. Since $0 < \alpha < 1/2$, then $(\log \alpha)/\log (1-\alpha) \geq -2 (\log 2)/\log (1-\alpha)$ or $\zeta \geq 2\xi$. Thus $2D(\xi) = D(2\xi) + 1 \leq D(\zeta) + 1$.

Finally assume $0 < F(\xi) < 1/2$ and $\alpha > 1/4$. Then $D(2\xi) = 2D(\xi) - 1$. Since $\alpha > 1/4$, then $\log \alpha > -2 \log 2$. Since $0 < \alpha < 1/2$, then $(\log \alpha)/\log (1-\alpha) < -2 (\log 2)/\log (1-\alpha)$, or $\zeta < 2\xi$. Thus $D(\zeta) + 1 \leq D(2\xi) + 1 = 2D(\xi)$.

The expression $\beta/(1-\alpha)$ is nonsymmetric in α and β. The

next theorem shows that the substitution of $\gamma(h)$ for β in $\beta/(1-\alpha)$ gives the best results in determining the order of a basis set from this inequality.

Theorem 3.54. If $0 < \alpha \leq \gamma < 1 - \alpha$, then $\alpha/(1-\gamma) \leq \gamma/(1-\alpha)$.

Proof. Let $f(x) = x(1-x)$ where x is real. Then $f(x)$ has a maximum at $x = 1/2$, is symmetric about $x = 1/2$, and is concave downward for $0 < x < 1$. Hence $\alpha(1-\alpha) \leq \gamma(1-\gamma)$ for $\alpha \leq \gamma \leq 1 - \alpha$, and the theorem follows.

Definition 3.55 [9]. The Erdös density α_1 of a set A is given by

$$\alpha_1 = \text{glb} \left\{ \frac{A(F)}{I^n(F)+1} \mid F \in \mathfrak{N} , A(F) < I^n(F) \right\}.$$

Definition 3.56. Let $X \subset I^n$. Then $\overline{X} = \{x \mid x \in I^n, x \notin X\}$.

Freedman [9] proved the following theorem.

Theorem 3.57 (Freedman). Let $A, B \subset I^n$. If $\overline{A+B} \neq \emptyset$, then $\gamma \geq \alpha_1 + \beta$.

We use this theorem to obtain a density theorem relating γ to α and β.

Theorem 3.58. If $\alpha + \beta < 1$, then $\gamma \geq (2/3)\alpha + \beta$.

Proof. If $\gamma = 1$, then $\gamma > \alpha + \beta \geq (2/3)\alpha + \beta$. Hence we assume $\gamma < 1$. Also we assume $\alpha > 0$ for otherwise the theorem is immediate. Thus $A(F) \geq 1$ for all $F \in \mathcal{K}$. Now $\overline{A + B} \neq \emptyset$ and so $\overline{A} \neq \emptyset$. Thus $A(F) < I^n(F)$, and so $I^n(F) \geq 2$. Hence

$$\frac{A(F)}{I^n(F)+1} = \frac{I^n(F)}{I^n(F)+1} \cdot \frac{A(F)}{I^n(F)} \geq \frac{2}{3} \frac{A(F)}{I^n(F)} .$$

By Definition 3.5 we have

$$\frac{A(F)}{I^n(F)+1} \geq \frac{2}{3} \alpha ,$$

and so it follows from Definition 3.55 that $\alpha_1 \geq (2/3)\alpha$. Finally by Theorem 3.57 we have $\gamma \geq \alpha_1 + \beta \geq (2/3)\alpha + \beta$.

Theorem 3.59. It follows from the density theorem, if $\alpha + \beta < 1$, then $\gamma \geq (2/3)\alpha + \beta$, that if $\gamma(h-1) < 1 - \alpha$ and $h \geq 2$, then $\gamma(h) \geq ((2h+1)/3)\alpha$.

Proof. We use induction on h. For $h = 2$ we have $\gamma(2) \geq (5/3)\alpha$ since $\gamma(1) = \alpha < 1 - \alpha$. Thus we assume the theorem holds for $h = k$ where $k \geq 1$ is fixed and assume $\gamma(k) < 1 - \alpha$. Since $\gamma(h)$ is a monotonically increasing function of h for $0 < \alpha < 1/2$ we have $\gamma(k-1) \leq \gamma(k) < 1 - \alpha$. Thus with sets A

and B replaced by A and kA respectively we have

$$\gamma(k+1) \geq \frac{2}{3}\alpha + \gamma(k)$$

$$\geq \frac{2}{3}\alpha + \frac{2k+1}{3}\alpha$$

$$= \frac{2(k+1)+1}{3}\alpha .$$

Theorem 3.60. If $0 < \alpha < 1/2$, then A is a basis for I^n and has order

$$K(\alpha) = D(\psi) + 1$$

where

$$\psi = \frac{3-4\alpha}{2\alpha} .$$

Proof. The real number $h = \psi$ is the root of the equation

$$\frac{2h+1}{3}\alpha = 1 - \alpha .$$

Hence let $h_o = D(\psi)$. Then $h_o \geq 2$ since $\psi > 1$. Hence if $\gamma(h_o-1) < 1 - \alpha$, then by Theorem 3.59 we have

$$\gamma(h_o) \geq \frac{2h_o+1}{3}\alpha$$

$$\geq \frac{2\psi+1}{3}\alpha$$

$$= 1 - \alpha .$$

Since $\gamma(h_o) + \alpha \geq 1 - \alpha + \alpha = 1$, then by Theorem 3.43 Part 2 we have $\gamma(h_o+1) = 1$. If $\gamma(h_o-1) \geq 1 - \alpha$, then $\gamma(h_o-1) + \alpha \geq 1$ and again by Theorem 3.43 Part 2 we have $\gamma(h_o) = 1$. Thus in either case $\gamma(h_o+1) = 1$. Finally by Theorem 3.43 Part 1 we have

$$K(\alpha) \leq h_o + 1 = D(\psi) + 1.$$

Theorem 3.61. If $0 < \alpha < 1/2$ and $1/2 \leq s < 1 - \alpha$, then A is a basis for I^n and has order

$$K(\alpha) \leq D(\frac{3s-\alpha}{2\alpha}) + D(\frac{3-3s-\alpha}{2\alpha}) .$$

Proof. Let the real number $h = \eta(s)$ be the root of the equation

$$\frac{2h+1}{3} \alpha = 1 - s.$$

Then $\eta(s) = (3-3s-\alpha)/2\alpha$ and $\eta(1-s) = (3s-\alpha)/2\alpha$. Let $h_1 = D(\eta(1-s))$ and $h_2 = D(\eta(s))$. Since $1/2 \leq s < 1 - \alpha$, then $\alpha < 1 - s \leq s$, and so $2\alpha < 3 - 3s - \alpha \leq 3s - \alpha$. Thus $\eta(1-s) \geq \eta(s) > 1$, and so $h_1 \geq h_2 \geq 2$. If $\gamma(h_1-1) < 1 - \alpha$, then $\gamma(h_2-1) < 1 - \alpha$. Then by Theorem 3.59 we have

$$\gamma(h_1) = \frac{2h_1+1}{3}\,\alpha$$

$$\geq \frac{2\eta(1-s)+1}{3}\,\alpha$$

$$= s,$$

and

$$\gamma(h_2) = \frac{2h_2-1}{3}\,\alpha$$

$$\geq \frac{2\eta(s)+1}{3}\,\alpha$$

$$= 1 - s.$$

Since $\gamma(h_1) + \gamma(h_2) \geq s + 1 - s = 1$, then by Theorem 3.43 Part 2 we have $\gamma(h_1+h_2) = 1$. If $\gamma(h_1-1) \geq 1 - \alpha$, then $\gamma(h_1-1) + \alpha \geq 1$ and again by Theorem 3.43 Part 2 we have $\gamma(h_1) = 1$. Thus in either case we have $\gamma(h_1+h_2) = 1$. Finally by Theorem 3.43 Part 1 we have

$$K(\alpha) \leq h_1 + h_2$$

$$= D(\eta(1-s)) + D(\eta(s))$$

$$= D(\frac{3s-\alpha}{2\alpha}) + D(\frac{3-3s-\alpha}{2\alpha}) .$$

This completes the proof.

The following theorem shows the bound for the order $K(\alpha)$ of A given by Theorem 3.60 is always as good as that given by Theorem 3.61.

Theorem 3.62. Let $n \geq 2$, $0 < \alpha < 1/2$ and $1/2 \leq s < 1 - \alpha$. If $\psi = (3-4\alpha)/2\alpha$ and $\eta(s) = (3-3s-\alpha)/2\alpha$, then

$$D(\eta(s)) + D(\eta(1-s)) \geq D(\psi) + 1$$

Proof.

$$\begin{aligned} D(\eta(s)) + D(\eta(1-s)) &\geq D(\eta(s)+\eta(1-s)) \\ &= D\left(\frac{3s-\alpha}{2\alpha} + \frac{3-3s-\alpha}{2\alpha}\right) \\ &= D\left(\frac{3-2\alpha}{2\alpha}\right) \\ &= D\left(\frac{3-4\alpha}{2\alpha}\right) + 1 \\ &= D(\psi) + 1. \end{aligned}$$

In the next theorem we compare the bounds for the order $K(\alpha)$ of A given by Theorem 3.47 and Theorem 3.60.

Theorem 3.63. If $0 < \alpha < 1/2$, $\zeta = (\log \alpha)/\log (1-\alpha)$, $\xi = -(\log 2)/\log (1-\alpha)$ and $\psi = (3-4\alpha)/2\alpha$, then $D(\psi) + 1 \leq D(\zeta) + 1$ and $D(\psi) + 1 \leq 2D(\xi)$.

It is interesting that while the bound given for $K(\alpha)$ by Theorem 3.60 is always at least as good as the bounds given by Theorems 3.47, 3.49 and 3.51, the fundamental density inequality on which Theorem 3.60 is based is incomparable with the fundamental density inequalities on which these other theorems are based.

Proof of Theorem 3.63. Since $0 < \alpha < 1/2$, then $3 - 4\alpha > 2\alpha > 0$ and $\log(1-\alpha) > \log \alpha$. But then $(3-4\alpha)\log(1-\alpha) > 2\alpha \log \alpha$, and so $(3-4\alpha)/2\alpha < (\log \alpha)/\log(1-\alpha)$. Hence $D(\psi) + 1 \leq D(\zeta) + 1$. Furthermore $3 - 2\alpha > 4\alpha > 0$ and $\log(1-\alpha) > \log(1/2)$. But then $(3-2\alpha)\log(1-\alpha) > -4\alpha \log 2$, and so $(3-2\alpha)/2\alpha < -2(\log 2)/\log(1-\alpha)$. Hence

$$\begin{aligned} D(\psi) + 1 &= D(\psi+1) \\ &= D\left(\frac{3-2\alpha}{2\alpha}\right) \\ &\leq D\left(\frac{-2 \log \alpha}{\log(1-\alpha)}\right) \\ &= D(2\xi) \\ &\leq 2D(\xi). \end{aligned}$$

We conclude this section by comparing the bound for $K(\alpha)$ given in Theorem 3.60 with that given in Theorem 3.64 below. The statement of Theorem 3.64 is identical to that of Theorem 3.38; the meaning is different because α is defined differently.

Theorem 3.64. If $0 < \alpha < 1/2$ and $n \geq 1$, then A is a basis for I^n and has order

$$K(\alpha) = nD\left(\frac{1}{\alpha}\right).$$

Proof. If we replace $\{A(L(x))/I^n L(x)) \mid L(x) \in \mathcal{C}\}$ by

$\{A(F)/I^n(F) \mid F \in \mathcal{K}\}$ in the proof of Lemma 3.37, we see that Lemma 3.37 is valid for α_K. Hence if we replace α by α_K in the proof of Theorem 3.38 we obtain a proof of Theorem 3.64.

Theorem 3.65. If $0 < \alpha < 1/2$, $n \geq 2$ and $\psi = (3-4\alpha)/(2\alpha)$, then $D(\psi) + 1 \leq nD(1/\alpha)$.

Proof. We have $(3-2\alpha)/2 < 2 \leq n$ and so

$$\psi + 1 = \frac{3-4\alpha}{2\alpha} + 1 = \frac{3-2\alpha}{2\alpha} < \frac{n}{\alpha}.$$

Hence

$$D(\psi) + 1 = D(\psi+1) \leq D(\frac{n}{\alpha}).$$

We have for real x by well known properties of the integer part function that $nD(x) = -nE(-x) \geq -E(-nx) = D(nx)$. Hence if we set $x = 1/\alpha$ we have

$$D(\psi) + 1 \leq D(\frac{n}{\alpha}) \leq nD(\frac{1}{\alpha}).$$

Section 3-5. Remarks

The proofs given in this chapter are algebraic in character and are based on fundamental density theorems. These density theorems are stated for a particular space, for example I or I^n, and for a particular density, for example α, α_C, or α_K. However a particular basis theorem is valid in any space and for any density in

which the needed fundamental density theorems are valid. Several densities and spaces are mentioned at the end of Section 3-1.

Freedman [9, 11] has given a generalized theory of density in which he replaces I^n by a particular type of Abelian semigroup. For a certain density and under a certain condition Theorem 3. 10 Parts 1, 2 and 3 hold but Parts 4 and 5 have not been proved valid. Furthermore Theorem 3. 57 has not been proved valid. In this case Theorems 3. 46, 3. 47 and part of Theorem 3. 53 are valid while later results of the chapter have not been proved valid. Under another condition Theorem 3. 10 Parts 1, 2 and 4 hold but Parts 3 and 5 along with Theorem 3. 57 have not been proved valid. Again, in certain cases Theorem 3. 10 Parts 1, 2 and 5 are valid. Finally there is a density and a condition under which Parts 1, 2, 3 and 4 of Theorem 3. 10 hold but Part 5 along with Theorem 3. 57 have not been proved valid.

The author has been unsuccessful in applying mixed density theorems to obtain significant results.

CHAPTER IV

SUMS OF SUBSETS OF A BOOLEAN ALGEBRA

Section 4-1. Introduction

This section with the exception of the last paragraph is introductory to both Chapter 4 and 5. We give definitions and state theorems of a preliminary nature.

In a Master's Thesis L. Damewood [5] suggested the extension of additive number theory to finite Boolean algebras and obtained some initial results. In Chapter 4 we present generalizations of Damewood's results and prove other addition theorems. In Chapter 5 we modify the sum of two sets.

To the author's knowledge the additive theory of the next two chapters is new except for the four theorems of Damewood, Theorems 4.15, 4.33, 5.3, and 5.4. Other known theorems are included such as background theorems, and a theorem of Sperner for which we give a new proof.

Definition 4.1 [2, p. 74]. A Boolean algebra can be defined as follows. Let an algebraic system be composed of a set M containing (at least) two special elements 1 and 0, and of two binary operations $+$ and $\cdot$ on M such that, for any elements a, b

and c of M,

a) $a + b = b + a$ $\qquad a \cdot b = b \cdot a$,

b) $a + a = a$ $\qquad a \cdot a = a$,

c) $a + (b+c) = (a+b) + c$ $\qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

d) $a + (a \cdot b) = a$ $\qquad a \cdot (a+b) = a$,

e) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$,

f) for each element a of M there is an element a' of M such that $a + a' = 1$ and $a \cdot a' = 0$.

If $\leq$ is defined by "$a \leq b$ if and only if $a + b = b$," then $(M, +, \cdot, 0, 1)$ is a Boolean algebra.

We will write M for the system $(M, +, \cdot, 0, 1)$ hereafter.

Definition 4.2. For each $a \in M$ the element a' is called the complement of a.

The following theorem is a collection of results obtainable from Definition 4.1. These are available in standard elementary texts on Boolean algebra [1, 2]. This theorem will be used without specific mention in the material of Chapters 4 and 5.

Theorem 4.3. Let $a, b, c \in M$. Then

1) $\leq$ is a partial ordering in M;

2) $a \leq b$ if and only if $a \cdot b = a$;

3) $a + (b \cdot c) = (a+b) \cdot (a+c)$;

4) for each $a \in M$, a' is unique;

5) $0' = 1$; $1' = 0$; $(a')' = a$;

6) $(a+b)' = a' \cdot b'$; $(a \cdot b)' = a' + b'$;

7) $0 + a = a = 1 \cdot a$; $0 \cdot a = 0$; $1 + a = a$.

Definition 4.4 [1, p. 62]. A field of sets is a family of subsets of a set U, which contains U and is closed under complements, unions and intersections.

The next two theorems provide a familiar setting for Boolean algebras and give a useful representation.

Theorem 4.5 [1, p. 201]. Any Boolean algebra M is isomorphic to a field of sets, ordered by set inclusion, where $+$, $\cdot$, 0, and 1 of M correspond to union, intersection, $\emptyset$ and U respectively of the field of sets.

When M is finite we can say more as follows.

Theorem 4.6 [2, p. 76]. Any finite Boolean algebra M is isomorphic to the set algebra of all the subsets of some finite set P, ordered by set inclusion where $+$, $\cdot$, 0, and 1 of M correspond to union, intersection, $\emptyset$ and P respectively of the set algebra.

Definition 4.7. Let the cardinality of $A \subset M$ be denoted by $|A|$.

The following theorem is available in standard texts on Boolean algebra [1, 2].

Theorem 4.8. Let M be a finite Boolean algebra and let M be isomorphic to the set algebra of all subsets of a set P. If $|P| = n$, then $|M| = 2^n$.

Definition 4.9. When M is represented by the set algebra of a finite set P, where $|P| = n$, denote M by $\mathfrak{B}_1^n$.

The following important principle of Boolean algebra theory will be used frequently.

Principle of Duality [1, p. 180]. Any valid statement of Boolean algebra theory remains valid if $+$ and $\cdot$ are interchanged.

The above statement means every concept definable in terms of $+$ and $\cdot$ must also be dualized. For instance, the dual of 0 is 1 and the dual of $\leq$ is $\geq$.

Definition 4.10. Let $b \in M$ and $L(b) = \{x \mid x \in M, x \leq b\}$. Then $L(b)$ is called the lower set of b.

Definition 4.11. Let i be finite and $M_i = \{b \mid b \in M, |L(b)| = 2^i\}$. Then M_i is called the ith level of M. Denote the ith level of $\mathfrak{B}_1^n$ by M_i also.

Definition 4.12. Let $b \in M$ and $U(b) = \{x \mid x \in M, x \geq b\}$. Then $U(b)$ is called the upper set of b.

We note that $U(b)$ is dual to $L(b)$.

Definition 4.13. Let $a \in M_1$. Then a is called an atom of M.

Definition 4.14. If every element of M except 0 can be expressed as a sum of atoms, then M is called an atomic Boolean algebra.

Definition 4.15. Let $M_d = \{b \mid b \in M, |U(b)| = 2\}$. If $b \in M_d$, then b is called a dual atom.

Definition 4.16. Let $a, b \in M$. If neither $a \leq b$ nor $b \leq a$, then a and b are incomparable. Let $a \perp b$ mean a and b are incomparable.

Definition 4.17. Let $A, B \subset M$. The sum $A + B$ and the product $A \cdot B$ of A and B are given by

$A + B = \{a + b \mid a \in A, b \in B\}$ and $A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$.

We note that $A + B$ is dual to $A \cdot B$.

Some of the theorems are more general than necessary. In such cases the increased generality does not make the proof

significantly more difficult and the resulting theory is more amenable to possible future generalizations. On the other hand, in some cases a proof uses the set algebra representation of Theorem 4.6. When any theorem of these chapters depends upon finiteness we will include $|M| = 2^n$ in the hypothesis.

In Section 4-2 we present cardinality conditions for an element to be in a sum or a product of subsets of a finite Boolean algebra. In Section 4-3 we determine the cardinality of $A + B$ and $A \cdot B$ in terms of the cardinality of A and B where A and B are subsets of M_1 or M_d in an atomic Boolean algebra.

Section 4-2. Cardinality Conditions for an Element to be in a Sum or Product

L. Damewood [5] proved the following theorem, for which we give a new proof.

Theorem 4.18 (Damewood). Let $|M| = 2^n$, $n \geq 1$, and $A, B \subset M$. If $|A| + |B| > 2^n$, then $1 \in A + B$.

Proof. We suppose that $1 \notin A + B$ and find a contradiction. Let $B^- = \{b' | b \in B\}$. We note that $|B^-| = |B|$. Now, if $a \in A \cap B^-$, then $a \in A$ and $a' \in B$, and so $a + a' = 1 \in A + B$. Thus $A \cap B^- = \emptyset$. However, then

$$|M| \geq |A \cup B^-|$$
$$= |A| + |B^-| - |A \cap B^-|$$
$$= |A| + |B|$$

which contradicts the hypothesis.

The remainder of this section generalizes Damewood's theorem. The dual of each theorem will be stated at the end of the section.

We first prove two lemmas.

Lemma 4.19. Let t be finite, $t \geq 1$, and $b \in M_t$. Then $L(b)$ with the operations of M is a Boolean algebra with unity b.

Proof. Let $a_1, a_2 \in L(b)$. Then $a_1 \leq b$ and $a_2 \leq b$. Thus $a_1 + a_2 \leq b$, and so $a_1 + a_2 \in L(b)$. Similarly $a_1 \cdot a_3 \in L(b)$. Let $a \in L(b)$ and $\bar{a} = b \cdot a'$. Then $\bar{a} \in L(b)$ and $a + \bar{a} = a + (b \cdot a') = (a+a') \cdot (a+b) = 1 \cdot b = b \in L(b)$. Furthermore $a \cdot \bar{a} = a \cdot (b \cdot a') = 0 \in L(b)$. Thus $\bar{a}$ is the complement of a relative to $L(b)$. All other properties are inherited from M and the lemma follows.

Lemma 4.20. Let $|M| = 2^n$, $n \geq 1$. If $b \in M_t$, $0 \leq t \leq n$, then b is represented by a set Q in $\mathfrak{B}_1^n$ where $|Q| = t$.

Proof. By Definition 4.11 we have that if $b \in M_t$, $0 \leq t \leq n$, then $|L(b)| = 2^t$. Let b be represented by the set Q in $\mathfrak{B}_1^n$.

Since $\mathfrak{B}_1^n$ is ordered by set inclusion then $|L(b)| = 2^t = |\{R | R \subset Q\}|$. Thus $|Q| = t$.

The following theorem shows Theorem 4.18 is, in a sense, best possible.

Theorem 4.21. Let $|M| = 2^n$, $n \geq 1$. There are sets $A, B \subset M$ for which $|A| + |B| = 2^n$ and $1 \notin A + B$.

Proof. Let $c \in M_{n-1}$ and $A = B = L(c)$. If $a \in A$ and $b \in B$, then by Lemma 4.19 we have $a + b \in L(c)$, and so $A + B = A$. Now $c < 1$ so $1 \notin A + B$. Finally, by Definition 4.11 we have $|A| = |B| = 2^{n-1}$, and so $|A| + |B| = 2 \cdot 2^{n-1} = 2^n$.

Lemma 4.22. If $A_1, A_2, A_3 \subset M$, then $A_1 + (A_2+A_3) = (A_1+A_2) + A_3$ and $A_1 + A_2 = A_2 + A_1$.

Proof. The operation $+$ in M is both associative and commutative.

Definition 4.23. Let $A_1, A_2, \ldots, A_h, h \geq 1$, be subsets of M. The sum of $A_1, A_2, \ldots, A_h$, denoted by $\Sigma_{i=1}^h A_i$ is A_1 if $h = 1$ and is given recursively by

$$\sum_{i=1}^{h} A_i = A_h + \sum_{i=1}^{h-1} A_i \quad \text{if} \quad h \geq 2.$$

Theorem 4.24. Let $|M| = 2^n$, $n \geq 1$, and $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$. If $\Sigma_{i=1}^{h} |A_i| > h \cdot 2^{n-1}$, then $1 \in \Sigma_{i=1}^{h} A_i$.

Proof. Since $\Sigma_{i=1}^{h} |A_i| > h \cdot 2^{n-1}$, then there is a set A_i for which $|A_i| > 2^{n-1}$. We may assume this set is A_1. Now, assume for each j, $2 \leq j \leq h$, that

$$|A_1| + |A_j| \leq 2^n.$$

Summing over j we have

$$(h-1)|A_1| + \sum_{j=2}^{h} |A_j| \leq (h-1)2^n.$$

Thus

$$\begin{aligned} \sum_{j=1}^{h} |A_j| &\leq (h-1)2^n - (h-2)|A_1| \\ &\leq (h-1)2^n - (h-2)2^{n-1} \\ &= h \cdot 2^{n-1}, \end{aligned}$$

which contradicts the hypothesis. Thus there is some j, $2 \leq j \leq h$, for which $|A_1| + |A_j| > 2^n$. We may assume $j = 2$. Then $|A_1| + |A_2| > 2^n$ and by Theorem 4.18 we have $1 \in A_1 + A_2$. Since $1 + a = 1$ for every $a \in M$, then $1 \in \Sigma_{i=1}^{h} A_i$.

The next theorem shows that Theorem 4.24 is, in a sense, best possible.

Theorem 4.25. Let $|M| = 2^n$, $n \geq 1$. There are sets $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$, for which $\Sigma_{i=1}^{h} |A_o| = h \cdot 2^{n-1}$ and $1 \notin \Sigma_{i=1}^{h} A_i$.

Proof. Let $c \in M_{n-1}$ and $A_i = L(c)$, $i = 1, 2, \ldots, h$. If $a_i \in A_i$, then $a_i \leq c$, $i = 1, 2, \ldots, h$, and so $\Sigma_{i=1}^{h} a_i \leq c$. Thus $\Sigma_{i=1}^{h} a_i \in L(c)$, and so $\Sigma_{i=1}^{h} A_i = L(c)$. Now $1 \notin L(c)$ and, by Definition 4.11, we have $\Sigma_{i=1}^{h} |A_i| = \Sigma_{i=1}^{h} |L(c)| = h \cdot 2^{n-1}$.

Next we extend Theorem 4.18 and Theorem 4.21 to an arbitrary element of M.

Theorem 4.26. Let $|M| = 2^n$, $n \geq 1$, and $A, B \subset M$. If $|A| + |B| > 2^{n+1} - 2^t$, $0 \leq t \leq n$, then $M_t \subset A + B$.

Proof. If $t = 0$, then $M_t = \{0\}$ and $|A| + |B| > 2^{n+1} - 1$ or $|A| + |B| \geq 2^{n+1}$. However, since $A, B \subset M$, then $|A| \leq 2^n$ and $|B| \leq 2^n$. Thus $|A| + |B| \leq 2^{n+1}$, and so $|A| + |B| = 2^{n+1}$. Then $A = B = M$ and $0 \in A + B$. Hence we assume $1 \leq t \leq n$. Let $c \in M_t$, $A' = A \cap L(c)$, and $B' = B \cap L(c)$. Since $L(c)$ and $M \setminus L(c)$ form a partition of M, then A' and $A \cap (M \setminus L(c))$ form a partition of A. Now $|L(c)| = 2^t$ so

$$|A| = |A'| + |A \cap (M \setminus L(c))|$$
$$\leq |A'| + |M \setminus L(c)|$$
$$= |A'| + 2^n - 2^t.$$

Similarly $|B| \leq |B'| + 2^n - 2^t$. Thus

$$|A'| + |B'| \geq |A| + |B| - 2(2^n - 2^t)$$
$$> 2^{n+1} - 2^t - 2^{n+1} + 2^{t+1}$$
$$= 2^t.$$

By Lemma 4.19, $L(c)$ is a Boolean algebra with unity c and, since $A', B' \subset L(c)$, by Theorem 4.18 we have $c \in A' + B' \subset A+B$.

The next theorem shows that Theorem 4.26 is, in a sense, best possible.

Theorem 4.27. Let $|M| = 2^n$, $n \geq 1$. There are sets $A, B \subset M$ for which $|A| + |B| = 2^{n+1} - 2^t$, $0 \leq t \leq n$, and $M^t \not\subset A + B$.

Proof. Let $t = 0$, $A = M$ and $B = M \setminus \{0\}$. Then $|A| + |B| = 2^n + 2^n - 1 = 2^{n+1} - 1$, but $0 \notin A + B$. Hence we suppose $1 \leq t \leq n$ and $c \in M_t$. Let $c_1 \in L(c) \cap M_{t-1}$ and $A = B = L(c_1) \cup (M \setminus L(c))$. Since $L(c_1) \subset L(c)$, then

$$|A| = |B| = |M| - |L(c)| + |L(c_1)|$$

$$= 2^n - 2^t + 2^{t-1}$$

$$= 2^n - 2^{t-1}.$$

Thus

$$|A| + |B| = 2^{n+1} - 2^t.$$

Finally, if $c \in A + B$, then $c = a + b$ where $a \in A$ and $b \in B$. Hence $a \leq c$, and so $a \in L(c)$. But then $a \notin M \setminus L(c)$ and so $a \in L(c_1)$. Similarly $b \in L(c_1)$. But then $a + b = c \in L(c_1)$ which contradicts $c_1 < c$. Thus $c \notin A + B$ and the theorem follows.

The following two theorems extend Theorem 4.24 and Theorem 4.25 to an arbitrary element of M.

Theorem 4.28. Let $|M| = 2^n$, $n \geq 1$, and $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$. If $\Sigma_{i=1}^{h} |A_i| > h(2^n - 2^{t-1})$, $1 \leq t \leq n$, then $M_t \subset \Sigma_{i=1}^{h} A_i$.

Proof. Let $c \in M_t$ and $A_i' = A \cap L(c)$, $i = 1, 2, \ldots, h$. Since $L(c)$ and $M \setminus L(c)$ form a partition of M, then A_i' and $A_i \cap (M \setminus L(c))$ form a partition of A_i for each i, $i = 1, 2, \ldots, h$. Now $|L(c)| = 2^t$ so

$$|A_i| = |A_i'| + |A_i \cap (M \setminus L(c))|$$

$$\leq |A_i'| + |M \setminus L(c)|$$

$$= |A_i'| + 2^n - 2^t$$

for each i, $i = 1, 2, \ldots, h$. Thus

$$\sum_{i=1}^{h} |A_i| \leq \sum_{i=1}^{h} |A_i'| + h(2^n - 2^t),$$

and so

$$\sum_{i=1}^{h} |A_i'| \geq \sum_{i=1}^{h} |A_i| - h(2^n - 2^t)$$

$$> h(2^n - 2^{t-1}) - h(2^n - 2^t)$$

$$= h \cdot 2^{t-1}.$$

Finally, $L(c)$ is a Boolean algebra with unity c, and so by Theorem 4.24 we have $c \in \Sigma_{i=1}^{h} A_i' \subset \Sigma_{i=1}^{h} A_i$.

The next theorem shows that Theorem 4.28 is, in a sense, best possible.

Theorem 4.29. Let $|M| = 2^n$, $n \geq 1$. There are sets $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$, for which $\Sigma_{i=1}^{h} |A_i| = h(2^n - 2^{t-1})$, $1 \leq t \leq n$, and $M_t \notin \Sigma_{i=1}^{h} A_i$.

Proof. Let $c \in M_t$, $c_1 \in L(c) \cap M_{t-1}$ and $A_i = L(c_1) \cup (M \setminus L(c))$, $i = 1, 2, \ldots, h$. Since $L(c_1) \subset L(c)$ we have

$$|A_i| = |L(c_1)| + |M| - |L(c)|$$

$$= 2^{t-1} + 2^n - 2^t$$

$$= 2^n - 2^{t-1}$$

for each i, $i = 1, 2, \ldots, h$. Thus

$$\sum_{i=1}^{h} |A_i| = h(2^n - 2^{t-1}).$$

Finally, if $c \in \Sigma_{i=1}^{h} A_i$, then $c = \Sigma_{i=1}^{h} a_i$ where $a_i \in A_i$, $i = 1, 2, \ldots, h$. Hence $a_i \leq c$ and so $a_i \in L(c)$, $i = 1, 2, \ldots, h$. But then $a_i \notin M \setminus L(c)$ and so $a_i \in L(c_1)$, $i = 1, 2, \ldots, h$. However then $c = \Sigma_{i=1}^{h} a_i \in L(c_1)$ which contradicts $c_1 < c$. Thus $c \notin \Sigma_{i=1}^{h} A_i$ and the theorem follows.

The following theorem gives a cardinality condition for 0 to be in an arbitrary sum of sets.

Theorem 4.30. Let $|M| = 2^n$, $n \geq 1$, and $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 1$. If $\Sigma_{i=1}^{h} |A_i| \geq h \cdot 2^n$, then $0 \in \Sigma_{i=1}^{h} A_i$.

Proof. Since $A_i \subset M$, then $|A_i| \leq 2^n$, $i = 1, 2, \ldots, h$, and

so $\Sigma_{i=1}^{h} |A_i| \leq h \cdot 2^n$. Since $\Sigma_{i=1}^{h} |A_i| \geq h \cdot 2^{n-1}$, then $\Sigma_{i=1}^{h} |A_i| = h \cdot 2^n$. Thus $|A_i| = 2^n$ and so $A_i = M$, $i = 1,2,\ldots,h$, and the theorem follows.

The next theorem shows that Theorem 4.30 is, in a sense, best possible.

Theorem 4.31. Let $|M| = 2^n$, $n \geq 1$. There are sets $A_i \subset M$, $i = 1,2,\ldots,h$, $h \geq 1$ for which $\Sigma_{i=1}^{h} |A_i| = h \cdot 2^n - 1$ and $0 \notin \Sigma_{i=1}^{h} A_i$.

Proof. Let $A_1 = M \setminus \{0\}$ and $A_i = M$, $i = 2,3,\ldots,h$. Then $\Sigma_{i=1}^{h} |A_i| = h \cdot 2^n - 1$ but $0 \notin \Sigma_{i=1}^{h} A_i$.

The following theorem shows the condition $h \geq 2$ in Theorem 4.24 and Theorem 4.28 is necessary.

Theorem 4.32. Let $|M| = 2^n$, $n > 1$. For each t, $t = 0,1,\ldots,n$, there is a set $A \subset M$ for which $|A| > 2^{n-1}$ and $M_t \not\subset A$.

Proof. For given t, $0 \leq t \leq n$, let $b \in M_t$, and let $A = M \setminus \{b\}$. Then $|A| = 2^n - 1 > 2^{n-1}$ and $M_t \not\subset A$.

We note that $t = 0$ cannot be included in Theorem 4.28 for $h \geq 3$ by observing that if we let $A_i = M$, $i = 1,\ldots,h-1$, and

$A_h = M \setminus \{0\}$, then $\Sigma_{i=1}^{h} |A_i| = h \cdot 2^n - 1 > h(2^n - (1/2))$ and $0 \notin \Sigma_{i=1}^{h} A_i$.

Damewood proves the following theorem in detail without the Principle of Duality. We prove the same theorem by the Principle of Duality.

Theorem 4.33 (Damewood). Let $|M| = 2^n$, $n \geq 1$, and $A, B \subset M$. If $|A| + |B| > 2^n$, then $0 \in A \cdot B$.

Proof. The dual of 1 is 0 and the dual of $A + B$ is $A \cdot B$. Applying the Principle of Duality to Theorem 4.18 proves the theorem.

Lemma 4.34. Let t be finite, $t \geq 1$, and $b \in M_t$. Then $U(b)$ with the operations of M is a Boolean algebra with zero b.

Proof. We have that the dual of $L(b)$ is $U(b)$ and the dual of unity is zero. Thus, applying the Principle of Duality to Lemma 4.19 gives the lemma.

Lemma 4.35. Let $|M| = 2^n$, $n \geq 1$. Then $b \in M_t$, $0 \leq t \leq n$, if and only if $|U(b)| = 2^{n-t}$.

Proof. Let $M = \mathfrak{B}_1^n$ where $1 \in M$ is represented by the set P and $|P| = n$. Then $b \in M_t$ is represented by a subset

Q of P where $|Q| = t$. Since the order relation $\leq$ in M corresponds to set inclusion in $\mathfrak{B}_1^n$, then

$$\begin{aligned} |U(b)| &= |\{R \mid R \subset P,\ Q \subset R\}| \\ &= |\{R \mid R = Q \cup T,\ T \subset (P \setminus Q)\}| \\ &\quad - |\{T \mid T \subset (P \setminus Q)\}|. \end{aligned}$$

Since $|P \setminus Q| = n - t$, then $|U(b)| = 2^{n-t}$.

To prove the converse we suppose that $b \in M_r$ where $r \neq t$. Then, by the above argument we have $|U(b)| = 2^{n-r}$ and $2^{n-r} \neq 2^{n-t}$.

The following lemma will be used frequently in the remainder of this section.

Lemma 4.36. Let $|M| = 2^n$, $n \geq 1$. Then the dual of M_t is M_{n-t}.

Proof. The dual of $M_t = \{b \mid |L(b)| = 2^t\}$ is $\{b \mid |U(b)| = 2^t\}$. By Lemma 4.35 we have $\{b \mid |U(b)| = 2^t\}$ is some level, which we assume to be M_s. Then, by Lemma 4.35 again we have that if $b \in M_s$, then $|U(b)| = 2^{n-s}$. Thus if $b \in M_s$, we have $2^t = |U(b)| = 2^{n-s}$, and so $s = n - t$.

We conclude this section with the dual theorems which follow by the Principle of Duality from the theorems starting with Theorem

4.21 and extending through Theorem 4.32.

Theorem 4.37. Let $|M| = 2^n$, $n \geq 1$. There are sets $A, B \subset M$ for which $|A| + |B| = 2^n$ and $0 \notin A \cdot B$.

Lemma 4.38. If $A_1, A_2, A_3 \subset M$, then $A_1 \cdot (A_2 \cdot A_3) = (A_1 \cdot A_2) \cdot A_3$ and $A_1 \cdot A_2 = A_2 \cdot A_1$.

Definition 4.39. Let $A_1, A_2, \ldots, A_h$, $h \geq 1$, be subsets of M. The product of $A_1, A_2, \ldots, A_h$, denoted by $\Pi_{i=1}^{h} A_i$, is A_1 if $h = 1$ and is given recursively by $\Pi_{i=1}^{h} A_i = A_h \cdot \Pi_{i=1}^{h-1} A_i$ if $h \geq 2$.

Theorem 4.40. Let $|M| = 2^n$, $n \geq 1$, and $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$. If $\Sigma_{i=1}^{h} |A_i| > h \cdot 2^{n-1}$, then $0 \in \Pi_{i=1}^{h} A_i$.

Theorem 4.41. Let $|M| = 2^n$, $n \geq 1$. There are sets $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$, for which $\Sigma_{i=1}^{h} |A_i| = h \cdot 2^{n-1}$ and $0 \notin \Pi_{i=1}^{h} A_i$.

Theorem 4.42. Let $|M| = 2^n$, $n \geq 1$ and $A, B \subset M$. If $|A| + |B| > 2^{n+1} - 2^t$, $0 \leq t \leq n$, then $M_{n-t} \subset A \cdot B$.

Theorem 4.43. Let $|M| = 2^n$, $n \geq 1$. There are sets $A, B \subset M$ for which $|A| + |B| = 2^{n+1} - 2^t$, $0 \leq t \leq n$, and $M_{n-t} \not\subset A \cdot B$.

Theorem 4.44. Let $|M| = 2^n$, $n \geq 1$, and $A_i \subset M$,

$i = 1, 2, \ldots, h$, $h \geq 2$. If $\Sigma_{i=1}^{h} |A_i| > h(2^n - 2^{t-1})$, $1 \leq t \leq n$, then $M_{n-t} \subset \Pi_{i=1}^{h} A_i$.

Theorem 4.45. Let $|M| = 2^n$, $n \geq 1$. There are sets $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 2$, for which $\Sigma_{i=1}^{h} |A_i| = h(2^n - 2^{t-1})$, $1 \leq t \leq n$, and $M_{n-t} \not\subset \Pi_{i=1}^{h} A_i$.

Theorem 4.46. Let $|M| = 2^n$, $n \geq 1$, and $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 1$. If $\Sigma_{i=1}^{h} |A_i| \geq h \cdot 2^n$, then $1 \in \Pi_{i=1}^{h} A_i$.

Theorem 4.47. Let $|M| = 2^n$, $n \geq 1$. There are sets $A_i \subset M$, $i = 1, 2, \ldots, h$, $h \geq 1$, for which $\Sigma_{i=1}^{h} |A_i| = h \cdot 2^n - 1$ and $1 \notin \Pi_{i=1}^{h} A_i$.

Theorem 4.48. Let $|M| = 2^n$, $n > 1$. For each t, $t = 0, 1, \ldots, n$, there is a set $A \subset M$ for which $|A| > 2^{n-1}$ and $M_t \not\subset A$.

Section 4-3. Sums and Products of Subsets of M_1 and M_d

In this section we restrict the investigation to the sum and product of two sets of atoms or dual atoms of an atomic Boolean algebra. We no longer require that M is finite but we do require that the subsets A and B of M are finite.

The following five lemmas for Boolean algebras are fundamental.

Lemma 4.49. If $a, b, c \in M$, $b \perp c$, and $a + b = a + c$, then $a \cdot b \neq a \cdot c$.

Proof. We assume $b \perp c$, $a + b = a + c$, and $a \cdot b = a \cdot c$, and find a contradiction. Since $a + b = a + c$, then $b \cdot (a+b) = b \cdot (a+c)$, and so $b = (a \cdot b) + (b \cdot c)$. Since $a \cdot b = a \cdot c$, then $b = (a \cdot c) + (b \cdot c) = (a+b) \cdot c$. Hence $b \cdot b = b \cdot (a+b) \cdot c$, and so $b = b \cdot c$. However $b \cdot c \leq c$, and so $b \leq c$ which contradicts our assumption. The lemma follows.

Lemma 4.50. If $A, B, C \subset M$, then $(A \cup B) + C = (A+C) \cup (B+C)$.

Proof. Let $x \in (A \cup B) + C$. Then $x = d + c$ where $d \in A \cup B$ and $c \in C$. Hence, $d \in A$ and $c \in C$, or $d \in B$ and $c \in C$. Finally, either $x = d + c \in A + C$ or $x = d + c \in B + C$, and so $x \in (A+C) \cup (B+C)$.

Let $x \in (A+C) \cup (B+C)$. Then $x \in A + C$ or $x \in B + C$. Then either $x = a + c$ where $a \in A$ and $c \in C$, or $x = b + c$ where $b \in B$ and $c \in C$. Thus, in either case we have $x \in (A \cup B) + C$.

Lemma 4.51. If $b, c \in M_1$ and $b \neq c$, then $b \perp c$, $b \cdot c = 0$, and $b + c \notin M_1$

Proof. By Definition 4.11 we see that if $b \in M_1$, then the equation $0 \leq x \leq b$ has exactly two solutions, namely $x = 0$ and $x = b$. First we suppose $b \perp c$ fails. Then either $b \leq c$ or $c \leq b$. If $b \leq c$ and $b \neq c$, then $b < c$. Thus $b = 0$ which contradicts $b \in M_1$. Similarly if $c \leq b$, then $c = 0$ which contradicts $c \in M_1$. Thus $b \perp c$. Next we suppose $b \neq c$ and $b \cdot c \neq 0$. Then, since $b \cdot c \leq b$, we have $b \cdot c = b$. However then $b = b \cdot c \leq c$ which contradicts $b \perp c$. Finally if $b + c \in M_1$, then $b \leq b + c$. Since $b \neq 0$, then $b = b + c$. Similarly $c = b + c$ and so $b = c$, a contradiction. This completes the proof.

Lemma 4.52. Let $a, b, c, d \in M_1$ and $a \neq b$. Then $a + c = b + d$ if and only if $a = d$ and $b = c$.

Proof. If $a = d$ and $b = c$, then $a + c = b + d$. Thus we assume $a \neq b$ and $a + c = b + d$. Then $a \cdot (a+c) = a \cdot (b+d)$, and so $a = (a \cdot b) + (a \cdot d)$. By Lemma 4.51 we have $a \cdot b = 0$, and so $a = a \cdot d$. Then, by Lemma 4.51 again we have $a = d$. Similarly $b \cdot (a+c) = b \cdot (b+d)$, and so $(a \cdot b) + (b \cdot c) = b$, or $b = b \cdot c$. Thus by Lemma 4.51 we have $b = c$ and the lemma follows.

Lemma 4.53. If $A, B, C \subset M_1$, then $(A+C) \cap (B+C) = ((A \cap B)+C) \cup ((A \cap C) + (B \cap C))$.

Note that the statement analogous to Lemma 4.50 is not valid even with M replaced by M_1: "If $A, B, C \subset M_1$, then $(A+C) \cap (B+C) = (A \cap B) + C$." For example, let $A = \{a, b\}$, $B = \{b, c\}$, and $C = \{a, c\}$.

Proof of Lemma 4.53. Let $x \in (A+C) \cap (B+C)$. Then $x \in A + C$ and $x \in B + C$, and so $x = a + c_1$ where $a \in A$, $c_1 \in C$, and $x = b + c_2$ where $b \in B$, $c_2 \in C$. Thus $a + c_1 = b + c_2$. We examine two cases.

Case 1. $a = c_1$.

Then $b + c_2 = a + c_1 = a$, and so $a \geq b$. Since $a, b \in M_1$ we have by Lemma 4.51 that $a = b$ or $a \perp b$. Hence $a = b$, and so $a \in A \cap B$. Finally $x = a + c_1 \in (A \cap B) + C$.

Case 2. $a \neq c_1$.

If $a = b$, then $a \in A \cap B$ and $c_1 \in C$ and so $x = a + c_1 \in (A \cap B) + C$. If $a = c_2$, then $a + c_1 = b + c_2 = a + b$. By Lemma 4.51 we have $a + b = a + c_1 \neq a$ and so $a \neq b$. Hence by Lemma 4.49 $b \perp c_1$ fails, and so by Lemma 4.51 we have $b = c_1$. Hence $a \in A \cap C$, $c_1 \in B \cap C$, and so $x = a + c_1 \in (A \cap C) + (B \cap C)$. Finally, if $a \neq b$ and $a \neq c_2$, then by Lemma 4.51 we have $a \cdot b = 0 = a \cdot c_2$. Since $a + c_1 = b + c_2$, then $a \cdot (a+c_1) = a \cdot (b+c_2)$ or $a = (a \cdot b) + (a \cdot c_2) = 0$ which contradicts

$a \in M_1$.

Hence $x \in ((A \cap B)+C) \cup ((A \cap C)+(B \cap C))$, and so $(A+C) \cap (B+C) \subset ((A \cap B)+C) \cup ((A \cap C)+(B \cap C))$.

Let $x \in ((A \cap B)+C) \cup ((A \cap B)+(B \cap C))$. Then $x \in (A \cap B) + C$ or $x \in (A \cap C) + (B \cap C)$. We again examine two cases.

Case 1. $x \in (A \cap B) + C$.

Then $x = d + c$ where $d \in A \cap B$ and $c \in C$. Hence $d \in A$ and $c \in C$, and so $x = d + c \in A + C$. Also $d \in B$ and again $c \in C$, and so $x = d + c \in B + C$. Hence $x \in (A+C) \cap (B+C)$.

Case 2. $x \in (A \cap C) + (B \cap C)$.

Then $x = d + e$ where $d \in A \cap C$ and $e \in B \cap C$, and so $d \in A$, $d \in C$, $e \in B$, and $e \in C$. Hence $x = d + e$ where $d \in A$ and $e \in C$, and so $x \in A + C$. Also $x = d + e$ where $d \in C$ and $e \in B$, and so $x \in B + C$. Hence $x \in (A+C) \cap (B+C)$.

Hence $((A \cap B)+C) \cup ((A \cap B)+(B \cap C)) \subset ((A+C) \cap (B+C))$ and the proof is complete.

We next obtain several cardinality theorems.

Theorem 4.54. Let $|A|$ and $|B|$ be finite. If $A, B \subset M_1$ and $A \cap B = \emptyset$, then $|A+B| = |A| \cdot |B|$.

Proof. For each $a \in A$, $b_i \in B$, $b_j \in B$, where $b_i \neq b_j$ we

have by Lemma 4.51 that $a \cdot b_i = 0 = a \cdot b_j$ and that $b_i \perp b_j$. Thus, by Lemma 4.49, $a + b_i \neq a + b_j$, and so $|\{a\}+B| = |B|$. By Lemma 4.53, if $a_i \in A$, $a_j \in A$ and $a_i \neq a_j$, we have

$$(\{a_i\}+B) \cap (\{a_j\}+B) = ((\{a_i\} \cap \{a_j\})+B) \cup (((\{a_i\} \cap B)+(\{a_j\} \cap B)) = \emptyset.$$

Hence $|A+B| = |\cup_{a \in A}(\{a\}+B)| = \Sigma_{a \in A}|\{a\}+B| = |A| \cdot |B|$.

Theorem 4.55. Let $|A|$ be finite. If $A \subset M_1$, then $|A+A| = (1/2)|A|(|A|+1)$.

Proof. We have $|A+A| = |\cup_{a \in A}(\{a\}+A)| = |A|^2 - \Delta$, where Δ is the number of repetitions of elements in the sum. By Lemma 4.53 we have that if $a_i \neq a_j$, then

$$(\{a_i\}+A) \cap (\{a_j\}+A) = ((\{a_i\} \cap \{a_j\})+A) \cup (((\{a_i\} \cap A)+(\{a_j\} \cap A))$$

$$= \{a_i + a_j\}.$$

Thus elements in the sum which are repeated occur just twice and are of the form $a_i + a_j$ where $a_i \neq a_j$. Thus $\Delta = \binom{|A|}{2}$ where $\binom{|A|}{2}$ is the binomial coefficient, and so

$$|A+A| = |A|^2 - \frac{1}{2}|A|(|A|-1)$$

$$= \frac{1}{2}|A|(|A|+1).$$

Theorem 4.56. Let $|A|$ and $|B|$ be finite. If $A, B \subset M_1$, then $|A+B| = |A| \cdot |B| - (1/2)|A \cap B|(|A \cap B|-1)$.

Proof. Let $C = A \cap B$. Then $A = C \cup (A \setminus C)$ and $B = C \cup (B \setminus C)$. Thus, by Lemma 4.50 we have

$$(1) \quad A + B = (C \cup (A \setminus C)) + (C \cup (B \setminus C)$$
$$= (C+(C \cup (B \setminus C))) \cup ((A \setminus C)+(C \cup (C \cup (B \setminus C))))$$
$$= (C+C) \cup (C+(B \setminus C)) \cup (C+(A \setminus C)) \cup ((A \setminus C)+(B \setminus C)).$$

Since $C \cap (C \setminus A) = \emptyset$ and $C \cap (C \setminus B) = \emptyset$, then by Lemma 4.52 the sets in this last union are pairwise disjoint. Thus, by Theorem 4.55 we have

$$(2) \quad |C + C| = \frac{1}{2}|C|(|C|+1) = \frac{1}{2}|C|^2 + \frac{1}{2}|C|.$$

By Theorem 4.54 we have

$$(3) \quad |C+(A \setminus C)| = |C| \cdot |A \setminus C| = |C|(|A|-|C|) = |A| \cdot |C| - |C|^2,$$

$$(4) \quad |C+(B \setminus C)| = |C| \cdot |B \setminus C| = |C|(|B|-|C|) = |B| \cdot |C| - |C|^2,$$

and

$$(5) \quad |(A \setminus C)+(B \setminus C)| = |A \setminus C| \cdot |B \setminus C| = (|A|-|C|)(|B|-|C|)$$
$$= |A| \cdot |B| + |C|^2 - |A| \cdot |C| - |B| \cdot |C|.$$

Substituting (2), (3), (4) and (5) into (1) we see that

$$|A+B| = |A| \cdot |B| + \frac{1}{2}|C| - \frac{1}{2}|C|^2$$
$$= |A| \cdot |B| - \frac{1}{2}|A \cap B|(|A \cap B|-1).$$

Note that Theorems 4.54 and 4.55 are special cases of Theorem 4.56. Theorem 4.57 is analogous to Theorem 4.56 but since the proof is simpler we do not first obtain special cases.

Theorem 4.57. Let $|A|$ and $|B|$ be finite and $A, B \subset M_1$. If $A = B$ and $|A| = 1$, then $|A \cdot B| = 1$. If either $A \neq B$ or both $A = B$ and $|A| \geq 2$, then $|A \cdot B| = |A \cap B| + 1$.

Proof. If $A = B = \{a\}$, then $A \cdot B = \{a\}$ and $|A \cdot B| = 1$. Thus we suppose either $A \neq B$ or both $A = B$ and $|A| \geq 2$. We show that $A \cdot B = (A \cap B) \cup \{0\}$. Let $x \in A \cdot B$. Then $x = a \cdot b$ where $a \in A$ and $b \in B$. If $a = b$, then $a \cdot b = a \in A \cap B$, and so $x = a \cdot b \in (A \cap B) \cup \{0\}$. If $a \neq b$, then by Lemma 4.51 we have $a \cdot b = 0$, and so $x = a \cdot b \in (A \cap B) \cup \{0\}$. Thus we see that $A \cdot B \subset (A \cap B) \cup \{0\}$. Now let $x \in (A \cap B) \cup \{0\}$. Then $x \in A \cap B$ or $x = 0$. If $x \in A \cap B$, then $x = x \cdot x \in A \cdot B$. If $x = 0$, then since $A \neq B$ or both $A = B$ and $|A| \geq 2$, there exists $a_o \in A$ and $b_o \in B$ such that $a_o \neq b_o$. Hence, by Lemma 4.51 we have that $x = 0 = a_o \cdot b_o \in A \ B$, and so $(A \cap B) \cup \{0\} \subset A \cdot B$. Thus $A \cdot B = (A \cap B) \cup \{0\}$. Finally since $0 \notin A \cap B$, then $|A \cdot B| = |(A \cap B) \cup \{0\}| = |A \cap B| + 1$.

We conclude this section with cardinality theorems for sums and products of subsets of M_d, the set of dual atoms.

Note that if $|M| = 2^n$, $n \geq 1$, then by Lemma 4.36 we have $M_d = M_{n-1}$.

Theorem 4.57. Let $|A|$ and $|B|$ be finite. If $A, B \subset M_d$, then $|A \bullet B| = |A| \cdot |B| - (1/2)|A \cap B|(|A \cap B| - 1)$.

Proof. The dual of M_1 is M_d and the dual of $A + B$ is $A \bullet B$. Thus applying the Principle of Duality to Theorem 4.56 proves the theorem.

Theorem 4.58. Let $|A|$ and $|B|$ be finite and $A, B \subset M_d$. If $A = B$ and $|A| = 1$, then $|A \bullet B| = 1$. If either $A \neq B$ or both $A = B$ and $|A| \geq 2$, then $|A \bullet B| = |A \cap B| + 1$.

Proof. The dual of M_1 is M_d and the dual of $A + B$ is $A \bullet B$. Thus applying the Principle of Duality to Theorem 4.57 proves the theorem.

CHAPTER V

A MODIFIED SUM OF SUBSETS OF A FINITE BOOLEAN ALGEBRA

Section 5-1. Introduction

In this chapter we use the definitions and some of the theorems of Chapter 4.

Theorem 5.1. Let $|M| = 2^n$, $n \geq 1$. There are subsets $A, B \subset M$ for which $|A + B| = 1$.

Proof. Let $c \in M$, $B = U(c)$ and $A = \{c'\}$. Then for $a \in A$ and $b \in B$ we have $a + b = c' + b \geq c' + c = 1$, and so $a + b = 1$. Thus $A + B = \{1\}$. The theorem follows.

The next theorem follows from Theorem 5.1 by use of the Principle of Duality.

Theorem 5.2. Let $|M| = 2^n$, $n \geq 1$. There are subsets $A, B \subset M$ for which $|A \cdot B| = 1$.

Damewood [5] proved the following two theorems for which we give different proofs.

Theorem 5.3 (Damewood). Given any positive integer m,

there is a finite Boolean algebra M with subsets A and B for which $|A| + |B| \geq |A + B| + m$.

Proof. For real x let $D(c)$ denote the least integer not less than x. For a given positive integer m, let $r = D((\log 2m)/\log 2)$, and $|M_1| = r$. Let $c \in M_1$, $B = U(c)$ and $A = \{c'\}$. If $x \in A + B$, then $x = b + c' \geq c + c' = 1$, and so $A + B = \{1\}$. Furthermore since $|M| = 2^r$ we have by Lemma 4.35 that $|A| + |B| = 1 + 2^{r-1}$. Substituting for r we obtain $|A| + |B| \geq 1 + m = |A + B| + m$. This completes the proof.

The next theorem follows from Theorem 5.3 and the Principle of Duality which Damewood did not use.

Theorem 5.4 (Damewood). Given any positive integer m, there is a finite Boolean algebra M with subsets A and B for which $|A| + |B| \geq |A \cdot B| + m$.

These four theorems indicate linear relationships between $|A|$, $|B|$ and $|A + B| = |\{a+b | a \in A, b \in B\}|$ would be extremely poor. In fact, without restrictions on A and B, the best we can say is $|A + B| \geq 1$ as is shown in Theorem 5.1.

Theorem 5.5. Let $|M| = 2^n$, $n \geq 1$. There are subsets $A, B \subset M$ for which $|A| > 1$, $|B| > 1$, and $A + B = A$,

Proof. Let $c \in M_t$, $1 \leq t \leq n-1$ and let $A = B = L(c)$. Then $|A| > 1$, $|B| > 1$, and by Lemma 4.19 we have that $A + B = A$.

Theorem 5.5 eliminates the consideration of a sum defined as in Definition 3.7, $A + B = A \cup B \cup \{a+b \mid a \in A, b \in B\}$, as the best we could say is $|A + B| \geq |A|$. We will define a modified sum of A and B which utilizes more of the intrinsic properties of a Boolean algebra. Lemma 4.49 suggests a possible choice as it indicates that when the number of elements of $A + B$ is small, then the number of elements of $A \cdot B$ is large. Thus we make the following definitions.

Definition 5.6. Let $A, B \subset M$. The * sum of A and B, denoted by $A * B$, is given by $A * B = (A+B) \cup (A \cdot B)$ where $A + B = \{a+b \mid a \in A, b \in B\}$ and $A \cdot B = \{a \cdot b \mid a \in A, b \in B\}$.

Definition 5.7. Let $A, B \subset M$. The o sum of A and B, denoted $A \circ B$, is given by $A \circ B = A \cup B \cup (A*B)$.

Note $A * B$ and $A \circ B$ are self dual. Note also that the forms of the sums of Definitions 2.3 and 3.7 are preserved.

In Section 5-2 we give cardinality theorems for $A * B$ and $A \circ B$ where A and B are subsets of M_1 and M_d of an atomic Boolean algebra. Thereafter we restrict the investigation to

$A * A$ where $A \subset M_t$ and M is finite. In Section 5-3 we give another representation for a finite Boolean algebra and a Boolean algebra isomorphism. In Section 5-4 we make a conjecture for $|A * A|$ and prove this conjecture in certain cases including all Boolean algebras M such that $|M| = 2^n$, $n = 1, 2, \ldots, 5$. In Section 5-5 we give a new proof of a 1930 theorem of E. Sperner [26] which establishes the maximal cardinality of a subset of incomparable elements of a finite Boolean algebra. Section 5-6 contains a collection of lemmas about Boolean algebras which have no particular application but could be of interest in further investigation of this problem. We complete this chapter with some research problems in Section 5-7.

Section 5-2. Sums of Subsets of Atoms and Dual Atoms

We use the results of Section 4-3 to derive expressions for $|A * B|$ and $|A \circ B|$. We first prove two lemmas.

Lemma 5.8. If $A, B \subset M_1$, then $(A+B) \cap (A \cup B) = (A \cap B)$.

Proof. Let $x \in (A+B) \cap (A \cup B)$. Then $x \in A + B$, and $x \in A$ or $x \in B$. Thus $x = a + b$ where $a \in A$, $b \in B$, and $x \in A$ or $x \in B$. If $x = a + b \in A$ then by Lemma 4.51 we have $a = b$, and so $x = a = b \in A \cap B$. Similarly if $x = a + b \in B$, then $x \in A \cap B$. Thus in either case $x \in A \cap B$.

Let $x \in A \cap B$. Then $x \in A \cup B$ and $x = x + x \in A + B$.

Thus $x \in (A+B) \cap (A \cup B)$. The lemma follows.

Lemma 5.9. If $A, B \subset M_1$, then $(A \cdot B) \cap (A \cup B) = (A \cap B)$.

Proof. Let $x \in (A \cdot B) \cap (A \cup B)$. Then $x \in A \cdot B$, and $x \in A$ or $x \in B$. Thus $x = a \cdot b$ where $a \in A$, $b \in B$, and $x \in A$ or $x \in B$. If $x = a \cdot b \in A$, then by Lemma 4.51 we have $a = b$, and so $x = a = b \in A \cap B$. Similarly if $x = a \cdot b \in B$, then $x \in A \cap B$. Thus, in either case $x \in A \cap B$.

Let $x \in A \cap B$. Then $x \in A \cup B$ and $x = x \cdot x \in A \cdot B$. Thus $x \in (A \cdot B) \cap (A \cup B)$. The lemma follows.

Theorem 5.10. Let $A, B \subset M_1$. If $A = B$ and $|A| = 1$, then $|A * B| = 1$. If $A \neq B$ or both $A = B$ and $|A| \geq 2$, then $|A * B| = |A| \cdot |B| - (1/2)|A \cap B|(|A \cap B| - 1) + 1$.

Proof. Suppose $A = B = \{a\}$. Then $A + B = \{a\} = A \cdot B$ and $|A * B| = |(A+B) \cup (A \cdot B)| = |\{a\}| = 1$. If $A \neq B$ or both $A = B$ and $|A| \geq 2$, then as we showed in the proof of Theorem 4.57, $A \cdot B = (A \cap B) \cup \{0\}$ where $0 \notin A \cap B$. Since $(A \cap B) \subset (A+B)$, then we have that

$$\begin{aligned} A * B &= (A+B) \cup (A \cdot B) \\ &= (A+B) \cup (A \cap B) \cup \{0\} \\ &= (A+B) \cup \{0\}. \end{aligned}$$

Hence by Theorem 4.56 and since $0 \notin A + B$ we have that

$$|A * B| = |A + B| + 1$$
$$= |A| \cdot |B| - \frac{1}{2}|A \cap B|(|A \cap B| - 1) + 1.$$

Theorem 5.11. Let $A, B \subset M_1$. If $A = B$ and $|A| = 1$, then $|A \circ B| = 1$. If $A \neq B$ or both $A = B$ and $|A| \geq 2$, then $|A \circ B| = |A| \cdot |B| + |A| + |B| - (1/2)|A \cap B|(|A \cap B| + 3) + 1$.

Proof. If $A = B = \{a\}$, then $A = B = A + B = A \cdot B = \{a\}$, and so $|A \circ B| = |A \cup B \cup (A+B) \cup (A \cdot B)| = 1$. If $A \neq B$ or both $A = B$ and $|A| \geq 2$, then we have by Lemmas 5.8 and 5.9 and Theorem 5.10 that

$$|A \circ B| = |A \cup B \cup (A*B)|$$
$$= |A \cup B| + |A*B| - |(A \cup B) \cap (A*B)|$$
$$= |A \cup B| + |A*B| - |(A \cup B) \cap ((A+B) \cup (A \cdot B))|$$
$$= |A \cup B| + |A*B| - |((A \cup B) \cap (A+B)) \cup ((A \cup B) \cap (A \cdot B))|$$
$$= |A \cup B| + |A*B| - |A \cap B|$$
$$= |A| + |B| - |A \cap B| + |A| \cdot |B| - \frac{1}{2}|A \cap B|(|A \cap B| - 1) + 1 - |A \cap B|$$
$$= |A| \cdot |B| + |A| + |B| - \frac{1}{2}|A \cap B|(|A \cap B| + 3) + 1.$$

The next two theorems follow from Theorems 5.10 and 5.11 and the Principle of Duality.

Theorem 5.12. Let $A, B \subset M_d$. If $A = B$ and $|A| = 1$, then $|A*B| = 1$. If $A \neq B$ or both $A = B$ and $|A| \geq 2$, then $|A*B| = |A| \cdot |B| - (1/2)|A \cap B|(|A \cap B| - 1) + 1$.

Theorem 5.13. Let $A, B \subset M_d$. If $A = B$ and $|A| = 1$, then $|A \circ B| = 1$. If $A \neq B$ or both $A = B$ and $|A| \geq 2$, then $|A \circ B| = |A| \cdot |B| + |A| + |B| - (1/2)|A \cap B|(|A \cap B| + 3) + 1$.

Section 5-3. Representation and Isomorphism Theorems

In Theorem 4.6 we observe that if $|A|$ is finite, then M is isomorphic to the set algebra of the set of all subsets of a finite set P. We now give a second representation which we will use frequently. The representation is standard.

Theorem 5.14 [1, p. 209]. Let $(\mathfrak{B}_2^n, +, \cdot, 0, 1)$ be an algebraic system where

$$\mathfrak{B}_2^n = \{x = (x^{(1)}, x^{(2)}, \ldots, x^{(n)}) \mid x^{(i)} \in \{0, 1\},\ i = 1, 2, \ldots, n\}$$

and $a + b = c$ and $a \cdot b = d$ are defined $c^{(i)} = \max\{a^{(i)}, b^{(i)}\}$ and $d^{(i)} = \min\{a^{(i)}, b^{(i)}\}$, $i = 1, 2, \ldots, n$. If $|M| = 2^n$, $n \geq 1$, then $(M, +, \cdot, 0, 1)$ is isomorphic to $(\mathfrak{B}_2^n, +, \cdot, 0, 1)$ where $+$, $\cdot$, 0, and 1 in M correspond to $+$, $\cdot$, $0 = (0, 0, \ldots, 0)$, and $1 = (1, 1, \ldots, 1)$ in $(\mathfrak{B}_2^n, +, \cdot, 0, 1)$ respectively.

We will denote $(\mathfrak{B}_2^n, +, \cdot, 0, 1)$ by $\mathfrak{B}_2^n$ and $x \in \mathfrak{B}_2^n$ by $x = (x^{(i)})$. We will call $x^{(i)}$ the ith position of x.

Definition 5.15. Let $|M| = 2^n$. When the representation $\mathfrak{B}_2^n$ is used for M we write $M = \mathfrak{B}_2^n$.

We next define an isomorphism in $\mathfrak{B}_2^n$.

Theorem 5.16. Let $I_{ij} : \mathfrak{B}_2^n \to \mathfrak{B}_2^n$ where $(x^{(1)}, \ldots, x^{(i)}, \ldots, x^{(j)}, \ldots, x^{(n)})I_{ij} = (x^{(1)}, \ldots, x^{(j)}, \ldots, x^{(i)}, \ldots, x^{(n)})$. That is the ith and jth positions of x are interchanged by I_{ij}. Then I_{ij} is a Boolean algebra isomorphism.

Proof. We observe I_{ij} is its own inverse, and so I_{ij} is a one to one, onto mapping. Furthermore, since $a + b$ and $a \cdot b$ are defined by position, then $(a+b)I_{ij} = aI_{ij} + bI_{ij}$ and $(a \cdot b)I_{ij} = aI_{ij} \cdot bI_{ij}$ follow immediately. Also $0I_{ij} = 0$ and $1I_{ij} = 1$. This completes the proof.

We will denote the ith level of $\mathfrak{B}_2^n$ by M_i.

Theorem 5.17. Let $|M| = 2^n$, $n \geq 1$. If $a \in M_t$, then $aI_{ij} \in M_t$, $0 \leq t \leq n$.

Proof. If $a \in M_t$, then a has t ones in its $\mathfrak{B}_2^n$ representation. Since I_{ij} is an interchange of positions, then aI_{ij} has

t ones, and so $aI_{ij} \in M_t$.

Section 5-4. A Conjecture and its Proof in Certain Cases

In this section we will consider a special case of the general problem. We restrict further investigation as follows.

Conjecture 5.18. Let $|M| = 2^n$, $n \geq 1$. If $A \subset M_t$, $0 \leq t \leq n$, then $|A * A| \geq 3|A| - 2$.

We prove this conjecture in a number of cases, including all Boolean algebras M such that $|M| = 2^n$, $n = 1, 2, \ldots, 5$. The general case remains unsolved. We note that the condition $A \subset M_t$ is reasonable as removal of this condition can cause the conjecture to fail. As an example, let $a \in M$ and $A = L(a)$.

Lemma 5.19. If $A \subset M_t$ and $|A| \geq 2$, then $\{A, (A+A) \setminus A, (A \cdot A) \setminus A\}$ forms a partition of $A * A$.

Proof. If $a, b \in M_t$, $a \neq b$, then $a + b > a$, for if $a + b = a$, then $b \leq a$. Hence $b < a$ which contradicts $a, b \in M_t$. Then by the Principle of Duality we have $a \cdot b < a$. Thus $a + b \in (A+A) \setminus A$, $a \cdot b \in (A \cdot A) \setminus A$ and $a \cdot a \in A$. Hence each of the sets is non-empty. It remains to show that $((A+A) \setminus A) \cap ((A \cdot A) \setminus A) = \emptyset$. Assume $x \in ((A+A) \setminus A) \cap ((A \cdot A) \setminus A)$. Then $x = a_1 + b_1 = a_2 \cdot b_2$ where $a_1, b_1, a_2, b_2 \in A$, $a_1 + b_1 \in (A+A) \setminus A$, and

$a_2 \cdot b_2 \in (A \cdot A) \setminus A$. If $a_1 = a_2$, then $a_1 + b_1 \geq a_1 = a_2 \geq a_2 \cdot b_2 = a_1 + b_1$, and so $a_1 + b_1 = a_1 \in A$, a contradiction. If $a_1 \neq a_2$, then $a_1 \perp a_2$ since $a_1, a_2 \in M_t$. However $a_1 \leq a_1 + b_1 = a_2 \cdot b_2 \leq a_2$, a contradiction. The lemma follows.

Theorem 5.20. Let $|M| = 2^n$, $n \geq 1$, and $A \subset M_t$. If $|A| = 1$ or $|A| = 2$, then $|A * A| = 3|A| - 2$.

Note that equality holds in Conjecture 5.18.

Proof of Theorem 5.20. If $|A| = 1$, then $A = \{a\} = A * A$. Thus $|A * A| = 3|A| - 2$. If $|A| = 2$, then $A = \{a, b\}$ and, by Lemma 5.19 we have $A * A = \{a+b, a, b, a \cdot b\}$. Thus $|A * A| = 4 = 3|A| - 2$.

Theorem 5.21. Let $|M| = 2^n$, $n \geq 1$ and $A \subset M_t$. If $|A| \geq 2$ and $|(A+A) \setminus A| = 1$, then $|(A \cdot A) \setminus A| = \binom{|A|}{2}$.

Proof. If $|A| = 2$, then $|(A+A) \setminus A| = 1 = |(A \cdot A) \setminus A|$. Thus we assume $|A| \geq 3$. If $a_i + a_j = a_i + a_k$ where i, j and k are all different, then since $a_j \perp a_k$ we have by Lemma 4.49 that $a_i \cdot a_j \neq a_i \cdot a_k$. Hence if $|A| = 3$, then we have $|(A \cdot A) \setminus A| = \binom{|A|}{2}$. Thus we assume $|A| \geq 4$. We suppose $a_i \cdot a_j = a_k \cdot a_m$ and find a contradiction. By hypothesis we have $a_i + a_k = a_i + a_m$ and $a_j + a_k = a_j + a_m$. Thus

$$a_k \cdot (a_i + a_k) = a_k \cdot (a_i + a_m)$$

and

$$a_k \cdot (a_j + a_k) = a_k \cdot (a_j + a_m),$$

and so

$$a_k = (a_i \cdot a_k) + (a_k \cdot a_m)$$

and

$$a_k = a_k \cdot (a_j + a_m).$$

Thus

$$(a_i \cdot a_k) + (a_k \cdot a_m) = a_k \cdot (a_j + a_m).$$

Since $a_i \cdot a_j = a_k \cdot a_m$, we have

$$(a_i \cdot a_k) + (a_i \cdot a_j) = a_k \cdot (a_j + a_m),$$

or

$$a_i \cdot (a_j + a_k) = a_k \cdot (a_j + a_m).$$

However, $a_i \leq a_i + a_j = a_j + a_k$ and $a_k \leq a_j + a_k = a_j + a_m$. Hence $a_i = a_k$, a contradiction. Thus we see $a_i \cdot a_j \neq a_k \cdot a_m$ and since no pair of products can be equal we have $|(A \cdot A) \setminus A| = \binom{|A|}{2}$. This completes the proof.

Theorem 5.22. Let $|M| = 2^n$, $n \geq 1$ and $A \subset M_t$. If $|A| \geq 2$ and $|(A \cdot A) \setminus A| = 1$, then $|(A + A) \setminus A| = \binom{|A|}{2}$.

Proof. The dual of $A + A$ is $A \cdot A$. Thus the theorem

follows from Theorem 5.21 and the Principle of Duality.

Theorem 5.23. Let $|M| = 2^n$, $n \geq 1$, and $A \subset M_t$. If $|A| = 3$, then $|A * A| \geq 3|A| - 2$.

Proof. If $|(A+A)\setminus A| = 1$, then by Theorem 5.21 we have $|(A \cdot A)\setminus A| = \binom{3}{2} = 3$. By Lemma 5.19 we have $|A * A| = |(A+A)\setminus A| + |A| + |(A \cdot A)\setminus A| = 1 + 3 + 3 = 7 = 3|A| - 2$ and the theorem is proved. Similarly by Theorem 5.22, if $|(A \cdot A)\setminus A| = 1$, then $|(A+A)\setminus A| = 3$, and so $|A * A| = 7 = 3|A|-2$. Thus we assume $|(A+A)\setminus A| \geq 2$ and $|(A \cdot A)\setminus A| \geq 2$. Then $|A * A| \geq 2 + 3 + 2 = 7 = 3|A| - 2$. This completes the proof.

Note that $|A * A| = 3|A| - 2$ if $|(A+A)\setminus A| = 1$ or $|(A \cdot A)\setminus A| = 1$. Thus the conjecture is, in a sense, best possible.

Definition 5.24. For $c \in (A*A)\setminus A$, let the degree of c, denoted $d(c)$, be given by $d(c) = |\{(a_i, a_j) | a_i, a_j \in A, a_i + a_j = c\}|$ or $d(c) = |\{(a_i, a_j) | a_i, a_j \in A, a_i \cdot a_j = c\}|$.

Theorem 5.25. Let $|M| = 2^n$, $n \geq 1$, $A \subset M_t$, and $\rho = \max\{d(c) | c \in (A*A)\setminus A\}$. If $\rho \leq |A|/2$, then $|A * A| \geq 3|A| - 2$.

Proof. By Lemma 5.19 we have that $|A * A| = |A| + |(A+A)\setminus A| + |(A \cdot A)\setminus A|$. Thus it remains to show

that $|(A+A)\setminus A| + |(A\cdot A)\setminus A| \geq 2|A| - 2$. Counting repetitions there are $\binom{|A|}{2}$ elements in each of $(A+A)\setminus A$ and $(A\cdot A)\setminus A$. Now $\binom{|A|}{2} = \Sigma_{c \in (A+A)\setminus A} d(c) \leq \rho\Sigma_{c \in (A+A)\setminus A} 1 = \rho|(A+A)\setminus A|$, and so $|(A+A)\setminus A| \geq \binom{|A|}{2}/\rho$. Similarly $|(A\cdot A)\setminus A| \geq \binom{|A|}{2}/\rho$. Hence

$$|(A+A)\setminus A| + |(A\cdot A)\setminus A| \geq \frac{2\binom{|A|}{2}}{\rho} \geq \frac{|A|(|A|-1)}{\frac{|A|}{2}} = 2|A| - 2.$$

This completes the proof.

The following theorems and lemmas establish that if $A \subset M_1$ and $A \subset M_2$, then $|A * A| \geq 3|A| - 2$. Following these we prove the conjecture for M where $|M| = 2^n$, $n = 1, 2, \ldots, 5$.

Theorem 5.26. Let $|M| = 2^n$, $n \geq 1$. If $A \subset M_1$, then $|A * A| \geq 3|A| - 2$.

Proof. Since $|A|$ is a positive integer we have that

$$(|A|-3)(|A|-2) \geq 0,$$

or

$$|A|^2 - 5|A| + 6 \geq 0.$$

Thus

$$|A|^2 + |A| + 2 \geq 6|A| - 4,$$

and so

(1) $$\frac{|A|^2+|A|+2}{2} \geq 3|A| - 2.$$

Now, by Theorem 5.10 we have

$$|A * A| = |A|^2 - \frac{1}{2}|A|(|A|-1) + 1$$

$$= \frac{|A|^2+|A|+2}{2}$$

Hence, by inequality (1) we have $|A * A| \geq 3|A| - 2$. This completes the proof.

Theorem 5.27. Let $|M| = 2^n$, $n \geq 1$. If $A \subset M_{n-1}$, then $|A * A| \geq 3|A| - 2$.

Proof. The dual of M_1 is M_{n-1}. Thus the theorem follows from Theorem 5.26 and the Principle of Duality.

Lemma 5.28. Let $|M| = 2^n$, $n \geq 1$. If $a \in M_r$, $b \in M_s$, and $a \cdot b \in M_t$, then $a + b \in M_{r+s-t}$.

Proof. Let $M = \mathbb{B}_2^n$. Since $a \cdot b \in M_t$, then a and b have 1 in the same t positions. Thus a has 1 in $r-t$ positions where b has 0, and b has 1 in $s-t$ positions where a has 0. Then $a + b$ has 1 in $t + (r-t) + (s-t) = r + s - t$ positions and 0 in all others. Thus

$a + b \in M_{r+s-t}$. Note that $r + s - t \leq n$. This completes the proof.

Lemma 5.29. Let $|M| = 2^n$, $n \geq 1$. If $a \in M_r$, $b \in M_s$ and $a + b \in M_t$, then $a \cdot b \in M_{r+s-t}$.

Proof. By Lemma 5.28 and the Principle of Duality we have, if $a \in M_{n-r}$, $b \in M_{n-s}$, and $a + b \in M_{n-t}$, then $a \cdot b \in M_{n+t-r-s}$. Let $r_1 = n - r$, $s_1 = n - s$, and $t_1 = n - t$. The lemma follows.

Lemma 5.30. Let $|M| = 2^n$, $n \geq 1$, $M = \mathbb{B}_2^n$, $A \subset M_t$, and $|A| \geq 2$. If for some m, $1 \leq m \leq n$, there exists $a_o \in A$ for which $a_o^{(m)} = 1$ and $a_i^{(m)} = 0$, for all $a_i \in A \setminus \{a_o\}$, then $|A * A| \geq |(A \setminus \{a_o\}) * (A \setminus \{a_o\})| + 3$.

Proof. Let $A' = A \setminus \{a_o\}$. If $|A| = 2$, then $A = \{a_o, a_1\}$ and $A' = \{a_1\}$. Then $A' + A' = A' = A' \cdot A'$, so $|A' * A'| = 1$. However, by Theorem 5.20 we have $|A * A| = 4$ and the theorem follows. Thus we assume $|A| > 2$.

Observe $a_o \notin A' * A'$. Since $a_i^{(m)} = a_j^{(m)} = 0$, $i \neq o \neq j$, then $(a_i + a_j)^{(m)} = 0$. However $(a_o + a_i)^{(m)} = 1$, and so in particular, $a_o + a_1 \notin A' * A'$. Thus it remains to show that at least one other element is in $A * A$ but not $A' * A'$. If there is some element $a_j \in A$, $j \neq 0$ for which $a_o + a_1 \neq a_o + a_j$, then using the above argument we have $a_o + a_j \notin A' * A'$ and the theorem follows. Thus we assume for all $a_i, a_j \in A$, $i \neq o \neq j$, that $a_o + a_i = a_o + a_j$. We

next show that $a_o + a_1 > a_i + a_j$, $i \neq o \neq j$.

Since $(a_o+a_1)^{(m)} = 1$ and $(a_i+a_j)^{(m)} = 0$, $i \neq o \neq j$, we have $a_o + a_1 \not< a_i + a_j$. Thus we assume $(a_o+a_1) \perp (a_i+a_j)$, $i \neq o \neq j$. Then there is q, $1 \leq q \leq n$, so that $(a_i+a_j)^{(q)} = 1$ and $(a_o+a_1)^{(q)} = 0$ for if not, then $a_i + a_j \leq a_o + a_1$. However then we see that $a_i^{(q)} = 1$ or $a_j^{(q)} = 1$. We may assume $a_i^{(q)} = 1$. Hence we have $(a_o+a_1)^{(q)} = 0$ and $(a_o+a_i)^{(q)} = 1$, which contradicts $a_o + a_1 = a_o + a_i$. Thus $(a_o+a_1) \perp (a_i+a_j)$ fails, and so $a_o + a_1 \geq a_i + a_j$. Finally, since $a_o + a_1 \neq a_i + a_j$, $i \neq o \neq j$, then $a_o + a_1 > a_i + a_j$.

Now, assume $a_o + a_1 \in M_r$. Then by Lemma 5.29 we have $a_o \cdot a_1 \in M_{2t-r}$. Also, since $a_i + a_j \in M_s$ where $s < r$, then $a_i \cdot a_j \in M_{2t-s}$ where $2t-s > 2t-r$. Hence $a_o \cdot a_1 \notin A' * A'$. This completes the proof.

Lemma 5.31. Let $|M| = 2^n$, $n \geq 1$, $M = \mathcal{B}_2^n$, $A \subset M_t$, and $|A| \geq 2$. If for some m, $1 \leq m \leq n$, there exists $a_o \in A$ for which $a_o^{(m)} = 0$ and $a_i^{(m)} = 1$, for all $a_i \in A \setminus \{a_o\}$, then $|A * A| \geq |(A \setminus \{a_o\}) * (A \setminus \{a_o\})| + 3$.

Proof. The dual of $a = (a^{(i)})$ is $b = (b^{(i)})$ where $b^{(i)} = 1 - a^{(i)}$, $1 \leq i \leq n$. Thus the lemma follows from Lemma 5.30 and the Principle of Duality.

Lemma 5.32. Let $|M| = 2^n$, $n \geq 1$, $M = \mathcal{B}_2^n$, $A \subset M_2$ and $|A| \geq 3$. If there exists $a_o \in A$ for which $a_o^{(m)} = 1$, $a_o^{(k)} = 1$, $m \neq k$, and there exist exactly one other element $a_1 \in A$ for which $a_1^{(m)} = 1$ and exactly one other element $a_2 \in A$ for which $a_2^{(k)} = 1$, then $|A * A| \geq |(A \setminus \{a_o\}) * (A \setminus \{a_o\})| + 3$.

Proof. Let $\delta_i = (\delta^{(1)}, \delta^{(2)}, \ldots, \delta^{(n)})$ where $\delta^{(j)} = 1$ if $j = i$, and $\delta^{(j)} = 0$ if $j \neq i$. Note that $\{\delta_i \mid 1 \leq i \leq n\} = M_1$. We observe $a_o \cdot a_1 = \delta_m$ and $a_o \cdot a_2 = \delta_k$. Furthermore, since no element of A other than a_o and a_1 has 1 in position m then $a_i \cdot a_j \neq \delta_m$, $\{i, j\} \neq \{0, 1\}$. Similarly no element of A other than a_o and a_2 has 1 in position k, and so $a_i \cdot a_j \neq \delta_k$, $\{i, j\} \neq \{0, 2\}$. Thus $\delta_m, \delta_k, a_1 \in A * A$, but $\delta_m, \delta_k, a_1 \notin (A \setminus \{a_o\}) * (A \setminus \{a_o\})$. This completes the proof.

Lemma 5.33. Let $|M| = 2^n$, $n \geq 1$, $M = \mathcal{B}_2^n$, $A \subset M_{n-2}$ and $|A| \geq 3$. If there exists $a_o \in A$ for which $a_o^{(m)} = 0$, $a_o^{(k)} = 0$, $m \neq k$, and there exist exactly one other element $a_1 \in A$ for which $a_1^{(m)} = 0$ and exactly one other element $a_2 \in A$ for which $a_2^{(k)} = 0$, then $|A * A| \geq |(A \setminus \{a_o\}) * (A \setminus \{a_o\})| + 3$.

Proof. The dual of M_2 is M_{n-2} and the dual of $a = (a^{(i)})$ is $b = (b^{(i)})$ where $b^{(i)} = 1 - a^{(i)}$, $1 \leq i \leq n$. Thus the lemma follows from Lemma 5.32 and the Principle of Duality.

Note Lemmas 5.29, 5.31, and 5.33 are not used explicitly. They are included for logical completeness.

Suppose we want to make the following statement fail. There is $a_o \in A$ for which $|A * A| \geq |(A \setminus \{a_o\}) * (A \setminus \{a_o\})| + 3$. Then it is necessary that A not satisfy the hypothesis of either Lemma 5.30 or Lemma 5.32. From Lemma 5.30 we have that if there is an element of A which has 1 in position k, then there is at least one other element in A which has a 1 in position k also. From Lemma 5.32 we have for $A \subset M_2$, $|A| \geq 3$ that each element of A must have one position in which it and at least two other elements have 1. These observations will be valuable in Theorems 5.35 and 5.36. The following lemma will be used in Theorem 5.37.

Lemma 5.34. Let $|M| = 2^n$, $n \geq 1$. If $A \subset M_2$ and $b \in ((A+A) \setminus A)$, then $d(b) \leq 3$.

Proof. Let $M = \mathbb{B}_2^n$. Then since $A \subset M_2$, we have that $b \in M_3$ or $b \in M_4$. If $b \in M_3$, then b has three 1's. There are $\binom{3}{2}$ ways of choosing two 1's from the three. Thus there are at most 3 elements of $A \subset M_2$ which are less than b. Hence at most $\binom{3}{2} = 3$ pairs of elements of A can have b as a sum. If $b \in M_4$ we show $d(b) \leq 3$ by exhibiting the pairs of elements of M_2 which can have b as a sum. Omitting commas, let $b = (1\ 1\ 1\ 1\ 0\ 0 \ldots 0)$. This choice is arbitrary as any element of

M_4 can be transformed to b by suitable choice of the isomorphisms I_{ij}. The only pairs of M_2 which sum to b are (1 1 0 0 0 . . . 0) and (0 0 1 1 0 0 . . . 0), (1 0 1 0 0 . . . 0) and (0 1 0 1 0 0 . . . 0), and (1 0 0 1 0 0 . . . 0) and (0 1 1 0 0 . . . 0). Thus $d(b) \leq 3$ in either case and the lemma follows.

In the proofs of the following two theorems we deal with $M_2 \subset \mathfrak{B}_2^5$. The only change required to go to a higher cardinality Boolean algebra is to add more zeros to each n-tuple. Since the proofs are carried out on the positions of the elements which contain 1, we note that these theorems are valid for an arbitrary finite Boolean algebra. The next three theorems establish if $A \subset M_2$, then $|A * A| \geq 3|A| - 2$. Since we deal with $M_2 \subset \mathfrak{B}_2^5$ we display the elements (omitting commas).

(1 1 0 0 0), (1 0 1 0 0), (1 0 0 1 0), (1 0 0 0 1), (0 1 1 0 0),

(0 1 0 1 0), (0 1 0 0 1), (0 0 1 1 0), (0 0 1 0 1), (0 0 0 1 1).

Observe, in each position there are four 1's and six 0's.

In our next two theorems we give a case study in $M_2 \subset \mathfrak{B}_2^5$. The construction of the case study isolates the cases, if any exist for which Lemmas 5.30 and 5.32 fail to apply for if either of these lemmas are applicable, then $|A * A| \geq |(A \setminus \{a_o\}) * (A \setminus \{a_o\})| + 3$. If $|A| = 4$, then $|A \setminus \{a_o\}| = 3$ and by Theorem 5.23 we have

that $|(A \setminus \{a_o\}) * (A \setminus \{a_o\})| \geq 3|A \setminus \{a_o\}| - 2$. Hence $|A * A| \geq 3|A \setminus \{a_o\}| - 2 + 3 = 3|A| - 2$. Having proved this we move to $|A| = 5$ and a similar statement.

Theorem 5.35. Let $|M| = 2^n$, $n \geq 1$, and $A \subset M_2$. If $|A| = 4$, then $|A * A| \geq 3|A| - 2$.

Proof. We let $M = \mathcal{B}_2^5$ and proceed according to the preceding remarks. Let $a_1 = (1\ 1\ 0\ 0\ 0)$ and $a_2 = (1\ 0\ 1\ 0\ 0)$. These choices are arbitrary in the sense that any other choice can be transformed to these by suitable I_{ij}. Furthermore, the first position requires two 1's. Suppose $a_3 = (0\ 1\ 1\ 0\ 0)$. Then any choice for a_4 will give the theorem as either the fourth or fifth position will have only one 1. Thus A satisfies the hypothesis of Lemma 5.30 and the theorem follows. Thus we suppose a_3 is some other element. Since we must have two 1's in the second position we can choose $(0\ 1\ 0\ 1\ 0)$ or $(0\ 1\ 0\ 0\ 1)$ and we observe the choices yield isomorphic sets with the isomorphism I_{45}. Hence let $a_3 = (0\ 1\ 0\ 1\ 0)$. Now any choice for element a_4 will give the theorem since $(0\ 0\ 1\ 1\ 0)$ will cause A to satisfy the hypothesis of Lemma 5.32 and any other element will cause A to satisfy the hypothesis of Lemma 5.30. This completes the proof.

Theorem 5.36. Let $|M| = 2^n$, $n \geq 1$, and $A \subset M_2$. If

$|A| = 5$, then $|A * A| \geq 3|A| - 2$.

Proof. We let $M = \binom{5}{2}$ and proceed according to the previous remarks. We first consider the case where all elements have 0 in the fifth position. Let $a_1 = (1\ 1\ 0\ 0\ 0)$ and $a_2 = (1\ 0\ 1\ 0\ 0)$. Since each element must have a position in which it and two other elements have 1's, let $a_3 = (1\ 0\ 0\ 1\ 0)$. The choice of $(0\ 1\ 1\ 0\ 0)$ or $(0\ 1\ 0\ 1\ 0)$ for a_4 gives isomorphic sets, so assume $a_4 = (0\ 1\ 1\ 0\ 0)$. We have to choose a_5 as $(0\ 1\ 0\ 1\ 0)$ or $(0\ 0\ 1\ 1\ 0)$. Again either choice gives isomorphic sets so assume $a_5 = (0\ 0\ 1\ 1\ 0)$. Observe this set does not satisfy the hypothesis of either Lemma 5.30 or 5.32. However $(a_4+a_5)^{(1)} = 0$ whereas $(a_i+a_j)^{(1)} = 1$ for $\{i, j\} \neq \{4, 5\}$. Also $(a_3 \cdot a_5)^{(4)} = 1$ whereas $(a_i \cdot a_j)^{(4)} = 0$ for $\{i, j\} \neq \{3, 5\}$. Thus the elements a_5, $a_4 + a_5$, $a_3 \cdot a_5$ are in $A * A$ but not in $(A \setminus \{a_5\}) * (A \setminus \{a_5\})$ and the theorem follows.

We begin again with $a_1 = (1\ 1\ 0\ 0\ 0)$, $a_2 = (1\ 0\ 1\ 0\ 0)$ and $a_3 = (1\ 0\ 0\ 1\ 0)$. We have exhausted the case where all the elements have 0 in the fifth position. Thus we assume a_4 has 1 in the fifth position. We first note that $a_4 = (1\ 0\ 0\ 0\ 1)$ would give the theorem for then the choice of a_5 could not put two 1's in each position and A would satisfy the hypothesis of Lemma 5.30. Thus we choose $a_4 = (0\ 1\ 0\ 0\ 1)$ and observe any other choice would give

isomorphic sets. Regardless of the choice of a_5 there will be one position with only one 1. Hence the theorem follows by Lemma 5.30. This completes the proof.

Theorem 5.37. Let $|M| = 2^n$, $n \geq 1$, and $A \subset M_2$. If $|A| \geq 6$, then $|A * A| \geq 3|A| - 2$.

Proof. Let $M = \mathbb{B}_2^n$. Since $|A| \geq 6$, $A \subset M_2$, and $|M_2| = \binom{n}{2}$ then $n \geq 4$. Suppose $n = 4$. Then $A = M_2$ and, as we show in Theorem 5.47, $|A * A| \geq 3|A| - 2$. Thus we assume $n \geq 5$. Suppose next that each position that has a 1 has at least two 1's. If there are only four such positions, then A is isomorphic to $M_2 \subset \mathbb{B}_2^4$ and the theorem follows from the above. Thus we assume there are at least five positions where each has at least two 1's. Then $|(A \cdot A) \setminus A| \geq 5$. Now, counting repetitions there are $\binom{|A|}{2}$ elements in $(A+A) \setminus A$. By Lemma 5.34 we have that $d(b) \leq 3$ for $b \in (A+A) \setminus A$. Then

$$\binom{|A|}{2} = \sum_{b \in (A+A)\setminus A} d(b) \leq 3|(A+A) \setminus A|,$$

and so $|(A+A) \setminus A| \geq (1/6)|A|(|A|-1)$. Thus

$$(1) \qquad |A * A| = |A| + |(A+A)\setminus A| + |(A\cdot A)\setminus A|$$

$$\geq |A| + \frac{|A|(|A|-1)}{6} + 5$$

$$= \frac{|A|^2+5|A|+30}{6}.$$

Now

$$(|A|-6)(|A|-7) \geq 0,$$

and so

$$|A|^2 - 13|A| + 42 \geq 0.$$

Thus

$$|A|^2 + 5|A| + 30 \geq 18|A| - 12,$$

and so

$$\frac{|A|^2+5|A|+30}{6} \geq 3|A| - 2.$$

Thus by inequality (1) we have $|A * A| \geq 3|A| - 2$. Finally suppose there is some position with only one 1, then by Lemma 5.30 and Theorem 5.36 the theorem follows for $|A| = 6$, then $|A| = 7$ and so on. This completes the proof.

Theorem 5.38. Let $|M| = 2^n$, $n \geq 1$. If $A \subset M_2$, then $|A * A| \geq 3|A| - 2$.

Proof. Theorems 5.20, 5.23, 5.35, 5.36, and 5.37 prove the theorem.

Theorem 5.39. Let $|M| = 2^n$, $n \geq 1$. If $A \subset M_{n-2}$, then $|A * A| \geq 3|A| - 2$.

Proof. The theorem follows from Theorem 5.38 and the Principle of Duality.

Theorem 5.40. Let $|M| = 2^n$, $n = 1, 2, \ldots, 5$. If $A \subset M_i$, $0 \leq i \leq n$, then $|A * A| \geq 3|A| - 2$.

Proof. Since isomorphic copies of each of the lower cardinality Boolean algebras exist as subsets of M, $|M| = 2^5$, we prove the theorem for this Boolean algebra only. If $A \subset M_o$, $A \subset M_1$ or $A \subset M_2$, then the theorem follows from Theorems 5.20, 5.26 and 5.38 respectively. If $A \subset M_3$, $A \subset M_4$ or $A \subset M_5$, then the theorem follows from Theorems 5.27, 5.39 and 5.20 respectively. This completes the proof.

We conclude this section with theorems about $A * A$ when $A = M_i$ for some i, $1 \leq i \leq n$, in a finite Boolean algebra.

Theorem 5.41. Let $|M| = 2^n$, $n \geq 1$. If $A = M_t$, $0 \leq t \leq n/2$, then $A * A = \cup_{i=0}^{2t} M_i$.

Proof. Let $M = B_2^n$. If $a, b \in A = M_t$, then a and b have t ones and $n-t$ zeros. Thus $a + b$ has no more than $2t$ ones, and so $a + b \in M_u$ where $0 \leq u \leq 2t$. Hence

$A * A \subset \cup_{i=0}^{2t} M_i$.

Let $\cup_{i=0}^{2t} M_i = (\cup_{i=0}^{t-1} M_i) \cup (M_t) \cup (\cup_{i=t+1}^{2t} M_i)$. We show each set in this union is contained in $A * A$. If $c \in M_t$, then $c = c + c \in (A+A) \subset A * A$. If $c \in M_k$ where $t+1 \leq k \leq 2t$, then c has k ones and $n-k$ zeros. By suitable choice of isomorphisms I_{ij} we may assume $c = (c^{(i)})$ where $c^{(i)} = 1$, $1 \leq i \leq k$ and $c^{(i)} = 0$, $k+1 \leq i \leq n$. Let $a \in A = M_t$ where $a^{(i)} = 1$, $1 \leq i \leq t$, and $a^{(i)} = 0$, $t+1 \leq i \leq n$. Also let $b \in A = M_t$ where $b^{(i)} = 1$, $k-(t-1) \leq i \leq k$, and $b^{(i)} = 0$ otherwise. Since $k-(t-1) \leq 2t-(t-1) = t + 1$, then $a + b = c \in (A+A) \subset A * A$. If $c \in M_j$ where $0 \leq j \leq t-1$, then again we may assume $c = (c^{(i)})$ where $c^{(i)} = 1$, $1 \leq i \leq j$ and $c^{(i)} = 0$, $j+1 \leq i \leq n$. Let $a \in A = M_t$ where $a^{(i)} = 1$, $1 \leq i \leq t$, and $a^{(i)} = 0$, $t+1 \leq i \leq n$. Also let $b \in A = M_t$ where $b^{(i)} = 1$, $1 \leq i \leq j$ and $n-(t-j-1) \leq i \leq n$, and $b^{(i)} = 0$ otherwise. Since $n-(t-j-1) \geq 2t-t+j+1 = t+j+1 > t$ then $a \cdot b = c \in A \cdot A \subset A * A$. This completes the proof.

Theorem 5.42. Let $|M| = 2^n$, $n \geq 1$. If $A = M_t$, $n/2 \leq t \leq n$, then $A * A = \cup_{i=2t-n}^{n} M_i$.

Proof. The dual of M_t is M_{n-t}. Thus, by Theorem 5.41 and the Principle of Duality we have, if $A = M_{n-t}$, $0 \leq t \leq n/2$,

then $A * A = \cup_{i=0}^{2t} M_{n-i}$. Let $t_1 = n-t$, and $i_1 = n-i$. Substituting in the above statement we have, if $A = M_{t_1}$, $n/2 \leq t_1 \leq n$, then $A * A = \cup_{i_1=n}^{n-2t} M_{i_1}$. The theorem follows.

Lemma 5.43. Let $|M| = 2^n$, $n \geq 1$. If $1 \leq t \leq n/2$, then $|M_{t-1}| < |M_t|$.

Proof. If $t \leq n/2$, then $2t \leq n$. Thus $t \leq n-t$, or $1 \leq (n-t)/t < (n-t+1)/t$. Thus we have

$$\frac{n!}{(n-t+1)!(t-1)!} < \frac{n-t+1}{t} \frac{n!}{(n-t+1)!(t-1)!} = \frac{n!}{(n-t)!t!}.$$

Hence

$$|M_{t-1}| = \frac{n!}{(n-t+1)!(t-1)!} < \frac{n!}{(n-t)!t!} = |M_t|.$$

Lemma 5.44. Let $|M| = 2^n$, $n \geq 1$. If $n/2 \leq t \leq n-1$, then $|M_t| > |M_{t+1}|$.

Proof. The dual of M_t is M_{n-t}. Thus, by Lemma 5.43 and the Principle of Duality we have, if $1 \leq t \leq n/2$, then $|M_{n-t+1}| < |M_{n-t}|$. Let $t_1 = n-t$. Substituting in the above statement we have, if $n/2 \leq t_1 \leq n-1$, then $|M_{t_1+1}| < |M_{t_1}|$.

Definition 5.45. For real x, let $E(x)$ denote the integer part of x.

Lemma 5.46. Let $|M| = 2^n$, $n \geq 1$. If $t = E(n/2)$, then $|M_t|$ is maximal.

Proof. If n is even, let $n = 2k$. Then $t = E(n/2) = k$ and the lemma follows from Lemmas 5.42 and 5.43. If n is odd, let $n = 2k + 1$. Then $t = E(n/2) = k$. We observe

$$|M_t| = \binom{2k+1}{k} = \binom{2k+1}{k+1} = |M_{t+1}|.$$

Thus by Lemma 5.43 we have $|M_{t-1}| < |M_t|$ for $1 \leq t \leq k$, and by Lemma 5.44 we have $|M_{t+1}| < |M_t|$ for $k+1 \leq t \leq n-1$. The lemma follows.

Theorem 5.47. Let $|M| = 2^n$, $n \geq 1$. If $A = M_t$, $0 \leq t \leq n$, then $|A * A| \geq 3|A| - 2$.

Proof. By Theorem 5.40 we can assume $n \geq 6$. We consider two cases.

Case 1. $0 \leq t \leq n/2$.

If $t = 0$, 1, or 2, then the theorem follows from Theorems 5.20, 5.26 and 5.38 respectively. Thus we assume $3 \leq t \leq n/2$. By Theorem 5.41 we have $A * A = \cup_{i=0}^{2t} M_i$, and so $|A * A| = \Sigma_{i=0}^{2t} |M_i|$.

If $3 \leq t \leq E(n/2) - 2$, then by Theorem 5.43 we have

$|M_t| < |M_{t+1}| < |M_{t+2}|$. Thus

$$|A * A| \geq |M_t| + |M_{t+1}| + |M_{t+2}| \geq 3|M_t| > 3|A| - 2.$$

Let $t = E(n/2) - 1$. If $n = 2r$, then $E(n/2) = r$, and so $t = r-1$. Furthermore

$$|M_{r-1}| = \binom{2r}{r-1} = \binom{2r}{r+1} = |M_{r+1}|.$$

Thus by Theorem 5.43 we have

$$|A * A| \geq |M_t| + |M_{t+1}| + |M_{t+2}| \geq 3|A| > 3|A| - 2.$$

If $n = 2r+1$, then $r = E(n/2)$, and so $t = r-1$. By Theorem 5.43 we have $|M_t| < |M_{t+1}|$. Furthermore

$$|M_{t+1}| = \binom{2r+1}{r} = \binom{2r+1}{r+1} = |M_{t+2}|.$$

Thus

$$|A * A| \geq |M_t| + |M_{t+1}| + |M_{t+2}| \geq 3|A| > 3|A| - 2.$$

Let $t = E(n/2)$. If $n = 2r$, then $t = E(n/2) = r$. By Theorem 5.41 we have $A * A = \bigcup_{i=0}^{2t} M_i = M$. Since $n \geq 6$, then $r \geq 3$. We show by induction on r, $r \geq 3$, that

$$|M| = 2^{2r} > 3|A| = \frac{3(2r)!}{r!r!}.$$

For $r = 3$ we have

$$2^6 = 64 > \frac{3(6!)}{3!3!} = 60.$$

Thus we assume $2^{2k} > 3\binom{2k}{k}$ is true for fixed k, $k \geq 3$. Now

$$4k^2 + 8k + 4 \geq 4k^2 + 6k + 2,$$

and so

$$4 \geq \frac{(2k+2)(2k+1)}{(k+1)^2}.$$

Thus

$$2^{2k+2} = 4 \cdot 2^{2k} > \frac{(2k+2)(2k+1)}{(k+1)^2} \frac{3(2k)!}{k!k!} = \frac{3(2k+2)!}{(k+1)!(k+1)!} = 3\binom{2(k+1)}{k+1}$$

and the inequality is true for $r \geq 3$. Thus for $n = 2r$, $r \geq 3$ we have

$$|A * A| = |M| = 2^n > 3|A| > 3|A| - 2.$$

If $n = 2r+1$, then $t = E(n/2) = r$. By Theorem 5.41 we have $A * A = \cup_{i=0}^{2t} M_i = M \setminus \{1\}$. Since $n \geq 6$ and n is odd, then $n \geq 7$, and so $r \geq 3$. We show by induction on r, $r \geq 3$, that

$$|M| - 1 = 2^{2r+1} - 1 > 3|A| = 3\frac{(2r+1)!}{(r+1)!\, r!}.$$

For $r = 3$ we have

$$2^7 - 1 = 127 > 3\frac{7!}{4!3!} = 105.$$

Thus we assume $2^{2k+1} - 1 > 3\binom{2k+1}{k}$ for fixed k, $k \geq 3$. Now,

$$4k^2 + 12k + 8 > 4k^2 + 10k + 6,$$

and so

$$4 \geq \frac{(2k+3)(2k+2)}{(k+2)(k+1)} .$$

Thus

$$2^{2k+3} - 1 > 4 \cdot 2^{2k+1} - 1 > \frac{3(2k+3)(2k+2)}{(k+2)(k+1)} \frac{(2k+1)!}{(k+1)!k!} = \frac{3(2k+3)!}{(k+2)!(k+1)!} ,$$

and the inequality is true for $r \geq 3$. Thus for $n = 2r+1$, $r \geq 3$, we have

$$|A * A| = |M| - 1 = 2^n - 1 > 3|A| > 3|A| - 2.$$

This completes Case 1.

Case 2. $n/2 \leq t \leq n$.

The dual of M_t is M_{n-t}. Letting $t = n-t_1$ in the theorem for Case 1 we have $n/2 \leq t_1 \leq n$, and so the theorem for Case 2 follows by the Principle of Duality. This completes the proof.

Section 5-5. A Proof of a Theorem of E. Sperner

We pose a more general conjecture.

Let $|M| = 2^n$, $n \geq 1$, and $A \subset M$. If $a_i \perp a_j$ for $a_i, a_j \in A$, $i \neq j$, then $|A * A| \geq 3|A| - 2$.

One method used by the author attempting to prove this conjecture was induction on $|A|$. Although prior attempts were fruitless, induction seems to offer the most optimistic course. In such a proof the theorem of this section determines the upper limit of the induction. This proof was completed after a literature search failed to disclose any information. Subsequently it was discovered that E. Sperner [26] proved the theorem in 1930. This proof is given since it relies upon graph theory whereas Sperner's proof is combinatorial. Furthermore, the techniques used in the proof could prove valuable in future investigations in the area of lattices.

We prove that a maximal set of incomparable elements of M is $M_{E(n/2)}$ where $|M| = 2^n$, $n \geq 1$.

The preliminary material, Definition 5.48 through Lemma 5.67, is available in Graph Theory by Ore [20]. The proofs are given as the material is collected from various parts of the book and specialized to our problem. The final theorems are the author's.

Definition 5.48. For $A \subset M$, let

$L'(A) = \{y | y \in M$ and there exists $x \in A$ for which $y < x\}$.

Definition 5.49. Let $\omega(A) = |A| - |L'(A)|$.

Lemma 5.50. Let $|M| = 2^n$, $n \geq 1$. If $A, B \subset M$, then

$|L'(A \cup B)| + |L'(A \cap B)| \leq |L'(A)| + |L'(B)|$.

Proof. We have that

$$L'(A\cap B) = \bigcup_{x\in A\cap B} L'(\{x\}) = \Big(\bigcup_{x\in A} L'(\{x\})\Big) \cup \Big(\bigcup_{x\in B} L'(\{x\})\Big)$$

$$= L'(A) \cup L'(B).$$

Also

$$L'(A\cap B) = \Big(\bigcup_{x\in A\cap B} L'(\{x\})\Big) \subset \Big(\Big(\bigcup_{x\in A} L'(\{x\})\Big) \cap \Big(\bigcup_{x\in B} L'(\{x\})\Big)\Big)$$

$$= L'(A) \cap L'(B).$$

Thus

$$|L'(A\cup B)| = |L'(A)\cup L'(B)| = |L'(A)| + |L'(B)| - |L'(A)\cap L'(B)|$$

$$\leq |L'(A)| + |L'(B)| - |L'(A\cap B)|.$$

Lemma 5.51. Let $|M| = 2^n$, $n \geq 1$. If $A, B \subset M$, then $\omega(A\cup B) + \omega(A\cap B) \geq \omega(A) + \omega(B)$.

Proof. We have

$$|A \cup B| + |A \cap B| = |A| + |B|. \tag{1}$$

By Lemma 5.50 we have

$$|L'(A\cup B)| + |L'(A\cap B)| \leq |L'(A)| + |L'(B)|. \tag{2}$$

Subtracting (2) from (1) we obtain

$$|A\cup B| - |L'(A\cup B)| + |A\cap B| - |L'(A\cap B)| \geq |A| - |L'(A)| + |B| - |L'(B)|.$$

Hence, by Definition 5.49 we have

$$\omega(A \cup B) + \omega(A \cap B) \geq \omega(A) + \omega(B).$$

Definition 5.52. Let $\omega(\emptyset) = 0$.

Definition 5.53. Let $\omega_o = \max \{\omega(A) \mid A \subset M\}$.

Lemma 5.54. $\omega_o \geq 0$.

Proof. $\emptyset \subset M$ and $\omega_o = \max \{\omega(A) \mid A \subset M\}$. Hence $\omega_o \geq 0$.

Definition 5.55. Let $A \subset M$. If $\omega(A) = \omega_o$, then A is called a critical set.

Lemma 5.56. Let $|M| = 2^n$, $n \geq 1$. If $A, B \subset M$ where A and B are critical sets, then $A \cap B$ and $A \cup B$ are critical sets.

Proof. By hypothesis we have $\omega(A) = \omega(B) = \omega_o$. Thus, by Lemma 5.51 we have $\omega(A \cup B) + \omega(A \cap B) \geq 2\omega_o$. However, since ω_o is maximal, this can occur only when $\omega(A \cup B) = \omega(A \cap B) = \omega_o$.

Lemma 5.57. Let $|M| = 2^n$, $n \geq 1$. There is a unique minimal critical set N contained in all others.

Proof. By Lemma 5.56, if A and B are critical sets,

then $A \cap B$ is a critical set. Let $N = \bigcap_{\omega(A)=\omega_o} A$.

Definition 5.58. Let $B \subset M$, $S(B) = B \cup L'(B)$. Then B is said to generate $S(B)$ and $S(B)$ is called a lower section.

Definition 5.59. Let $B_o \subset M$. Then B_o is called a minimal generating set if $S(B_o)$ cannot be generated by any proper subset of B_o.

Lemma 5.60. Let $|M| = 2^n$, $n \geq 1$, and B_o be a minimal generating set. If $b_1, b_2 \in B_o$, then $b_1 \perp b_2$.

Proof. Let $b_1, b_2 \in B_o$, $b_1 < b_2$. Then $b_1 \in L'(B_o \setminus \{b_1\})$. Thus $L'(B_o \setminus \{b_1\}) = L'(B_o)$. Hence $S(B_o) = S(B_o \setminus \{b_1\})$ which contradicts B_o is a minimal generating set. A similar argument contradicts $b_2 < b_1$. Hence $b_1 \perp b_2$.

Lemma 5.61. Let $|M| = 2^n$, $n \geq 1$, and $B_o, B_1 \subset M$. If B_o and B_1 are minimal generating sets and $B_o \cup L'(B_o) = B_1 \cup L'(B_1)$, then $B_o = B_1$.

Proof. We suppose $B_o \neq B_1$ and find a contradiction. By Definition 5.59 we have that $B_o \subset B_1$, and so there is $b_o \in B_o$ such that $b_o \notin B_1$. Thus since $B_o \subset B_1 \cup L'(B_1)$ we have $b_o \in L'(B_1)$. Thus there is $b_1 \in B_1$ such that $b_o < b_1$. But then by Lemma 5.60 we see that $b_1 \notin B_o$. Thus, since

$B_1 \subset B_o \cup L'(B_o)$ we have that $b_1 \in L'(B_o)$. Thus there is $b_2 \in B_o$ such that $b_1 < b_2$. Hence $b_o < b_1 < b_2$ where $b_o, b_2 \in B_o$ which contradicts Lemma 5.60. The lemma follows.

Lemma 5.62. Let $|M| = 2^n$, $n \geq 1$, and $A \subset M$. If A is a critical set, then A is a lower section.

Note that if A is a lower section then there is a set $B \subset M$ such that $A = S(B) = B \cup L'(B)$. Then

$$\begin{aligned} A \cup L'(A) &= B \cup L'(B) \cup L'(B \cup L'(B)) \\ &= B \cup L'(B) \cup L'(B) \cup L'(L'(B)) \\ &= B \cup L'(B) \cup L'(B) \cup L'(B) \\ &= B \cup L'(B). \end{aligned}$$

Thus $A = S(A)$. Hence A is a lower section if and only if $A = S(A)$.

Proof of Lemma 5.62. We assume A is a critical set and that A is not a lower section, that is $A \neq A \cup L'(A)$. Then for some $a \in A$ there is $b \in M$ such that $b < a$ and $b \notin A$. Hence $L'(\{b\}) \subset L'(A)$. Furthermore, since $\omega(A) = |A| - |L'(A)|$ we see

$$\omega(A\cup\{b\}) = |A\cup\{b\}| - |L'(A\cup\{b\})|$$
$$= |A| + 1 - |L'(A)|$$
$$= \omega(A) + 1.$$

This contradicts the hypothesis that A is a critical set and the lemma follows.

Lemma 5.63. Let $|M| = 2^n$, $n \geq 1$ and $A \subset M$. If A is a critical set, then $A \setminus L'(A)$ generates $S(A) = A$.

Proof. By Lemma 5.62 $S(A) = A$, and so we need to show $A \setminus L'(A)$ generates A. Let $a \in A$. Then either there is an $a_1 \in A$ such that $a < a_1$ or for every $a_i \in A$ we have $a \not< a_i$. Suppose $a < a_1$. Either $a_1 \in A \setminus L'(A)$ or there is an $a_2 \in A \setminus L'(A)$ such that $a_1 < a_2$. If $a_1 \notin A \setminus L'(A)$, then $a < a_1 < a_2 \in A \setminus L'(A)$. Also, if $a_1 \in A \setminus L'(A)$, then $a < a_1 \in A \setminus L'(A)$. Thus in either case we have $a \in L'(A \setminus L'(A))$. If $a \not< a_i$ for every $a_i \in A$, then $a \in A \setminus L'(A)$. Hence $A \subset (A \setminus L'(A)) \cup L'(A \setminus L'(A))$.

Suppose next that $x \in (A \setminus L'(A)) \cup L'(A \setminus L'(A))$. If $x \in A \setminus L'(A)$, then $x \in A$. Thus we assume $x \in L'(A \setminus L'(A))$. Then $x \in L'(A) \subset A$ because A is a lower section. Hence $(A \setminus L'(A)) \cup L'(A \setminus L'(A)) \subset A$.

Thus $S(A \setminus L'(A)) = A$ and $A \setminus L'(A)$ generates A.

Lemma 5.64. Let $|M| = 2^n$, $n \geq 1$, and $A, B_o \subset M$. If A is a critical set and B_o is the minimal generating set of A, then $B_o = A \setminus L'(A)$.

Proof. By Lemma 5.63 $A \setminus L'(A)$ generates A, and so that $A \setminus L'(A)$ is minimal remains to be shown. Suppose $A_1 \subsetneq A \setminus L'(A)$, and $A = A_1 \cup L'(A_1)$. Then there is an $a \in A \setminus L'(A)$ such that $a \notin A_1$. Thus $a \in L'(A_1)$; and so there is an $a_1 \in A_1$ such that $a < a_1$. However, then $a \in L'(A)$ and so $a \notin A \setminus L'(A)$ which is a contradiction. Thus $A \setminus L'(A) = B_o$ by Definition 5.59.

Lemma 5.65. Let $|M| = 2^n$, $n \geq 1$. If $B_o \subset M$ and B_o consists of pairwise incomparable elements, then $|B_o| \leq \omega_o$.

Proof. Let B denote the lower section generated by B_o, that is $B = B_o \cup L'(B_o)$. Then B_o is a minimal generating set. Hence $B_o \cap L'(B_o) = \emptyset$, and so $L'(B_o) = L'(B)$. Finally

$$|B_o| = |B| - |L'(B_o)| = |B| - |L'(B)| = \omega(B) \leq \omega_o.$$

Lemma 5.66. Let $|M| = 2^n$, $n \geq 1$. If A is a critical set of M, and B_o is the minimal generating set of A, then $|B_o| = \omega_o$.

Proof. By Lemma 5.64 we have $B_o = A \setminus L'(A)$. By Lemma 5.62 A is a lower section, and so $L'(A) \subset A$. Hence $|B_o| = |A| - |L'(A)| = \omega_o$.

Lemma 5.67. Let $|M| = 2^n$, $n \geq 1$. A critical set of M has a unique minimal generating set B_o where

1) The elements of B_o are pairwise incomparable;

2) The cardinality $|B_o|$ of B_o is maximal.

Proof. The lemma follows from Lemmas 5.60, 5.61, 5.65, and 5.66.

The remainder of this section is the application of these lemmas to determine the cardinality of the maximal set of incomparable elements.

Definition 5.68. Let $M = \mathbb{B}_2^n$, $n \geq 1$, and $T : \mathbb{B}_2^n \to \mathbb{B}_2^n$ where $(a^{(1)}, a^{(2)}, \ldots, a^{(n)})T = (a^{(n)}, a^{(1)}, a^{(2)}, \ldots, a^{(n-1)})$.

Lemma 5.69. Let $M = \mathbb{B}_2^n$. $T : \mathbb{B}_2^n \to \mathbb{B}_2^n$ is a Boolean algebra isomorphism.

Proof. T is the composition of appropriate isomorphisms I_{ij} as given in Theorem 5.16. The lemma follows.

Lemma 5.70. Let $M = \mathbb{B}_2^n$, $n \geq 1$, and $A \subset \mathbb{B}_2^n$. If

$T(A) = \{aT \mid a \in A\}$, then $|A| = |T(A)|$. If A is a critical set, then $T(A)$ is a critical set.

Proof. If $a, b \in A$ and $a \neq b$, then $aT, bT \in T(A)$ and $aT \neq bT$. Thus $|A| = |T(A)|$. Furthermore $|L'(A)| = |T(L'(A))| = |L'(T(A))|$. If A is a critical set, then $|A| - |L'(A)| = \omega_o$, and so $|T(A)| - |L'(T(A))| = \omega_o$. Hence $T(A)$ is a critical set.

Theorem 5.71. Let $|M| = 2^n$, $n \geq 1$. Then $\omega_o = \max |M_j|$.

Proof. Let A be the minimal critical set of M and let B_o be the minimal generating set of A. We show that $B_o \subset M_j$ for some j, $0 \leq j \leq n$. The theorem will then follow from Lemmas 5.66 and 5.67.

Assume $B_o \not\subset M_j$ for any j where $0 \leq j \leq n$. By Lemma 5.62 A is a lower section. Thus we let $A = B_o \cup L'(B_o)$. Let $j = \max \{i \mid M_i \cap B_o \neq \emptyset\}$. Now $M_j = (B_o \cap M_j) \cup (M_j \setminus B_o)$. By choice of j we have $T^{-1}(M_j \setminus B_o) \neq \emptyset$. Furthermore $T^{-1}(M_j \setminus B_o) \cap B_o \neq \emptyset$, for if so, then $M_j \setminus B_o = T^{-1}(M_j \setminus B_o)$. However, T is a cyclic permutation of M_j and no proper subset of M_j is mapped onto itself by a cyclic permutation. Thus there is $c \in T^{-1}(M_j \setminus B_o) \cap B_o$, and so there is $cT \in M_j \setminus B_o$ such that $c \in B_o$. If $cT \in A$ then $cT \in L'(B_o)$ and so there is $b \in B_o$

such that $b > cT$. Since $cT \in M_j$, then $b \in M_k$ where $k > j$ which contradicts the choice of j. Thus $cT \notin A$.

By Lemma 5.70 we have that $T(A)$ is a critical set. Hence $A \cap T(A) = A$ as A is the minimal critical set. However, $cT \notin A$, $c \in A$ and $|A| = |T(A)|$. Hence $A \cap T(A) \neq A$ which contradicts the choice of A. Thus $B_o \subset M_j$.

Theorem 5.72 (Sperner). The maximum number of elements in a set of incomparable elements of $M = \mathfrak{B}_1^n$ is $\binom{n}{j}$ where $j = E(n/2)$.

Proof. The maximum number is ω_o by Lemmas 5.65, 5.66, and 5.67. The theorem now follows from Theorem 5.71 and Lemma 5.46.

Section 5-6. Miscellaneous Theorems

The following lemmas were proved in the course of the investigation of this problem. These could be of interest in a further study.

Lemma 5.73. If $b \in (A+A) \setminus A$, and $a \leq b$, then there exists $a_1 \in A$ for which $a + a_1 \leq b$.

Proof. Since $b \in (A+A) \setminus A$, then there exists $a_1, a_2 \in A$ such that $a_1 + a_2 = b$. Since $a \leq b$, then $a + (a_1+a_2) = a+b = b$, and so $(a+a_1) + (a+a_2) = b$. Thus $a + a_1 \leq b$.

Lemma 5.74. If $b \in (A \cdot A) \setminus A$, and $a \geq b$, then there exists $a_1 \in A$ for which $a \cdot a_1 \geq b$.

Proof. The dual of $A + A$ is $A \cdot A$, the dual of $\leq$ is $\geq$, and the dual of $a + b$ is $a \cdot b$. Thus the lemma follows from Lemma 5.73 and the Principle of Duality.

Lemma 5.75. Let $|M| = 2^n$, $n \geq 1$. If $a_1 \in M_i$, $a_2 \in M_j$, $1 \leq i < j \leq n-1$, then there exists $a_3 \in M_j$ such that $a_2 \perp a_3$ and $a_1 \leq a_3$.

Proof. Since $1 \leq i < j \leq n-1$, then $j \geq 2$, and so $n \geq 3$. Thus $|U(a_1) \cap M_j| \geq 2$ which is easily obtained using either representation of M. Hence $U(a_1) \cap (M_j \setminus \{a_2\}) \neq \emptyset$. Let $a_3 \in U(a_1) \cap (M_j \setminus \{a_2\})$. Then $a_2 \perp a_3$ and $a_1 \leq a_3$.

Lemma 5.76. Let $|M| = 2^n$, $n \geq 1$. If $a_1 \in M_i$, $a_2 \in M_j$, $1 \leq i < j \leq n-1$, then there exists $a_3 \in M_i$ such that $a_1 \perp a_3$ and $a_2 \geq a_3$.

Proof. Since $1 \leq i < j \leq n-1$, then $j \geq 2$, and so $n \geq 3$. Thus $|L(a_2) \cap M_i| \geq 2$ which is easily obtained using either representation of M. Hence $L(a_2) \cap (M_i \setminus \{a_1\}) \neq \emptyset$. Let $a_3 \in L(a_j) \cap (M_i \setminus \{a_1\})$. Then $a_1 \perp a_3$ and $a_2 \geq a_3$.

Lemma 5.77. Let $|M| = 2^n$, $n \geq 1$, $a_1 \in M_i$, $a_2 \in M_j$,

$1 \leq i < j \leq n-1$ and $a_1 \perp a_2$. If $a_1 + a_2 = b_1$ and $a_1 \cdot a_2 = b_2$, then there exists $a_3 \in M_j$ such that $a_2 \perp a_3$, $a_2 + a_3 = b_1$ and $a_2 \cdot a_3 \geq b_2$.

Proof. Let $a_3 \in L(b_1) \cap U(a_1) \cap M_j$. Then $a_3 \leq b_1$, $a_3 \geq a_1$, and so $a_3 + a_2 = a_3 + a_1 + a_2 = a_3 + b_1 = b_1$. Furthermore $a_3 \cdot a_2 = (a_3+a_1) \cdot a_2 = (a_3 \cdot a_2) + (a_1 \cdot a_2) = (a_3 \cdot a_2) + b_2$ and so $a_3 \cdot a_2 \geq b_2$.

Lemma 5.78. Let $|M| = 2^n$, $n \geq 1$, $a_1 \in M_i$, $a_2 \in M_j$, $1 \leq i < j \leq n-1$ and $a_1 \perp a_2$. If $a_1 \cdot a_2 = b_1$ and $a_1 + a_2 = b_2$, then there exists $a_3 \in M_i$ such that $a_1 \perp a_3$, $a_1 \cdot a_3 = b_1$ and $a_1 + a_3 \leq b_2$.

Proof. Let $a_3 \in U(b_1) \cap L(a_2) \cap M_j$. Then $a_3 \geq b_1$, $a_3 \leq a_2$, and so $a_3 \cdot a_1 = a_3 \cdot a_2 \cdot a_1 = a_3 \cdot b_1 = b_1$. Furthermore $(a_3+a_1) = (a_3 \cdot a_2) + a_1 = (a_3+a_1) \cdot (a_2+a_1) = (a_3+a_1) \cdot b_2$. Thus $a_1 + a_3 \leq b_2$.

Section 5.7. Research Problems

We conclude this chapter with a short list of problems relating to sums of subsets of a Boolean algebra. We mention problems related to specific sections.

1) Section 4-2. Find cardinality conditions so that

$M_j \subset \Sigma_{i=1}^{h} A_i$ but $M_{j+1} \cap \Sigma_{i=1}^{h} A_i = \emptyset$.

2) Section 4-2. Find cardinality conditions so that $M_j \subset \Sigma_{i=1}^{h} A_i$ where conditions such as $A_i \cap A_j = \emptyset$ prevail.

3) Section 4-3. Extend the results of this section to higher levels of M.

4) Section 4-3. Extend the results of this section to an arbitrary Boolean algebra.

5) Section 5-2. Extend the results of this section to higher levels.

6) Section 5-3. Extend the result of this section to an arbitrary Boolean algebra.

7) Section 5-4. Prove the conjecture in a finite Boolean algebra.

8) Section 5-4. Extend the results to higher levels, and thereby to Boolean algebras of higher cardinality.

9) Section 5-4. Extend the results to an atomic Boolean algebra.

10) Section 5-4. Investigate the sum of other sets. For example $A * B$ where $A \cap B = \emptyset$ or $A * B$ where A and B are disjoint linearly ordered subsets of M.

11) Section 5-5. Study the stronger conjecture.

BIBLIOGRAPHY

1. Abbott, James C. Sets, lattices, and Boolean algebras. Boston, Allyn and Bacon, 1969. 282 p.

2. Arnold, B. H. Logic and Boolean algebra. Englewood Cliffs, Prentice-Hall, 1962. 144 p.

3. Besicovitch, A. S. On the density of the sum of two sequences of integers. Journal of the London Mathematical Society 10:246-248. 1935.

4. Chowla, I. A theorem on the addition of residue classes. Quarterly Journal of Mathematics, Oxford Series 8:99-102. 1937.

5. Damewood, Leroy M. Proofs of the $\alpha + \beta$ theorem based on Mann's transformation. Master's thesis. Corvallis, Oregon State University, 1960. 58 numb. leaves.

6. Davenport, H. On addition of residue classes. Journal of the London Mathematical Society 10:30-32. 1935.

7. Dyson, F. A theorem on the densities of sets of integers. Journal of the London Mathematical Society 20:8-14. 1945.

8. Erdös, Paul. On the asymptotic density of the sum of two sequences. Annals of Mathematics 43:65-68. 1942.

9. Freedman, Alan R. A general theory of density in additive number theory. Ph.D. thesis. Corvallis, Oregon State University, 1965. 125 numb leaves.

10. _____ An inequality for the density of the sum of two sets of vectors in n-dimensional space. Pacific Journal of Mathematics 19:265-267. 1966.

11. _____ Some generalizations in additive number theory. Journal für die reine und angewandte Mathematik 235:1-19. 1969.

12. Halberstam, H. and K. F. Roth. Sequences. Vol. 1. Oxford, Oxford University Press, 1966. 290 p.

13. Hardy, G. and E. Wright. The theory of numbers. 3d ed. Oxford, Oxford University Press, 1954. 419 p.

14. Kasch, Friedrich. Wesentliche Komponenten bei Gitterpunktmengen. Journal für die reine und angewandte Mathematik 197:208-215. 1957.

15. Kvarda, Betty. On densities of sets of lattice points. Pacific Journal of Mathematics 13:611-615. 1963.

16. Landau, E. Die Goldbachsche Vermutung und der Schnirelmannsche Satz. Nachtrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse. Fachgruppe II, 1930, p. 255-276.

17. Mann, Henry B. A proof of the fundamental theorem on the density of sums of sets of positive integers. Annals of Mathematics (2)43:523-527. 1942.

18. _____ On the products of sets of group elements. Canadian Journal of Mathematics 4:64-66. 1952.

19. _____ Addition theorems. New York, John Wiley, 1965. 114 p.

20. Ore, Oystein. Theory of graphs. Providence, American Mathematical Society, 1962. 270 p. (American Mathematical Society Colloquium Publications. Vol. XXXVIII)

21. Ostmann, H.-H. Additive Zahlentheorie. Berlin, Springer-Verlag, 1956. 236 p.

22. Pillai, S. Generalization of a theorem of Davenport on the addition of residue classes. Proceedings of the Indian Academy of Sciences 6:179-180. 1937.

23. Schnirelmann, L. Über additive Eigenschaften von Zahlen. Annales d'Institut polytechnique, Novočerkask 14:3-28. 1930.

24. _____ Über additive Eigenschaften von Zahlen. Mathematische Annalen 107:649-690. 1933.

25. Schur, Issai. Über den Begriff der Dichte in der additiven Zahlentheorie. Sitzungberichte der Preussischen Akademie der Wissenschaften. Physikalisch-Mathematische Klasse. 1936, p. 269-297.

26. Sperner, E. Über einen kombinatorischen Satz von Macauley und seine Anwendungen auf die Theorie der Polynomideale. Hamburg Universitat Mathematisches Seminar Abhandlungen 7:149-163. 1930.

27. Stalley, Robert. A modified Schnirelmann density. Pacific Journal of Mathematics 5:119-124. 1955.