THE UNIQUENESS OF THE NORDSTROM-ROBINSON AND THE GOLAY BINARY CODES

Thesis for the Degree of Ph. D.
MICHIGAN STATE UNIVERSITY
STEPHEN LEE SNOVER
1973

This is to certify that the

thesis entitled

The Uniqueness of the
Nordstrom-Robinson and Golay Binary Codes

presented by

Stephen Lee Snover

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics

L. M. Kelly
Major professor

Date Aug 1, 1973

O-7639

ABSTRACT

THE UNIQUENESS OF THE
NORDSTROM-ROBINSON AND THE GOLAY BINARY CODES

By

Stephen Lee Snover

In this thesis a code is considered to be any collection of vectors in $V(n,2)$, the vector space of n-dimensions over $GF(2)$. Two codes are considered to be equivalent if one can be obtained from the other by (a) a translation, i.e. adding a fixed vector of $V(n,2)$ to each code vector and/or (b) a permutation of the n fixed basis vectors of $V(n,2)$, i.e. the n coordinate positions of all the vectors. The notation (n,M,d) refers to a code of M vectors chosen from $V(n,2)$ so that the minimum Hamming distance between any pair of code vectors is d.

It is shown in this thesis that the codes given by the notation $(15,256,5)$, $(16,256,6)$, $(23,2^{12},7)$, and $(24,2^{12},8)$ are unique up to equivalence, and are the Nordstrom-Robinson code, its parity check extension code, the Golay binary code, and its extension, resp. Note that the uniqueness of the Golay code is proved without assuming linearity.

The key to the uniqueness proof lies in the fact that the minimun non-zero weight vectors in each of these codes are elements in a t-design: the sets of weight 5 and 6

vectors in the Nordstrom-Robinson code and its extension give rise to $4\text{-}(2,5,15)$ and $4\text{-}(3,6,16)$ designs while the sets of weight 7 and 8 code vectors in the Golay code and its extension form $S(4,7,23)$ and $S(5,8,24)$ Steiner systems. After discussing a new tool for the analysis of t-designs, called generalized block intersection numbers and a new definition, t-designs with $d \geq d_0$, i.e. t-designs which can be embedded in codes with minimum distance d_0, it is shown that the structure of each of these designs fixes the structure of the corresponding code. It follows that the proof of the uniqueness of the code up to an equivalence is reduced to showing that the corresponding minimum weight vector t-design is unique up to a permutation of the n coordinate positions.

The $4\text{-}(3,6,16)$ design with $d \geq 6$ generated by the weight 6 vectors in the extended Nordstrom-Robinson $(16,256,6)$ code is called the XNR-design and plays a fundamental role in showing the uniqueness of all the designs in question. In the first place, the XNR-design is shown to be unique by showing that any such design may always be embedded in $V(4,2)$ and then by showing that within $V(4,2)$ the design can only be constructed in one way, up to an automorphism of $V(4,2)$. Since the constructive proof of the XNR-design within $V(4,2)$ actually involves $PG(3,2)$, the uniqueness of both the Nordstrom-Robinson code and its extension follows.

Fr

ossibl

Steiner

mbers

SL(4,2

owing

niquel

cordin

ased o

roved

esign

niquen

f the

llow.

t is a

ode ex

rbitra

In

his th

f V(n

roups

.e. A

6, is

xtende

sed in

lassic

From the uniqueness of the XNR-design, it is also possible to conclude the uniqueness of the $S(4,7,23)$ Steiner system. Both the generalized block intersection numbers and the fact that a subgroup isomorphic to A_7 of $PSL(4,2)$ is 1-transitive on lines of $PG(3,2)$ aid in showing that the XNR-design builds the $S(4,7,23)$ design uniquely, up to an arbitrary permutation of the 7 added coordinates. Witt [40] proved the uniqueness of $S(4,7,23)$ based on the geometry of $PG(2,5)$, while the same result is proved here based on $PG(3,2)$ and the fact that the XNR-design is unique within this geometry.) Finally, from the uniqueness of $S(4,7,23)$, the uniqueness of $S(5,8,24)$ and of the Golay code and its extension, up to equivalence, follow. Because these proofs proceed from the XNR-design, it is actually shown that the extended Nordstrom-Robinson code extends to the Golay binary code uniquely, up to an arbitrary permutation of the added coordinates.

In order to tackle the coding theory problem basic to this thesis, concepts from t-designs, the finite geometries of $V(n,2)$ and $PG(n-1,2)$, and permutation and automorphism groups are used. In particular, it is shown that $A_7 + T(4)$, i.e. A_7 extended by the elementary abelian group of order 16, is the automorphism group of both the XNR-design and the extended Nordstrom-Robinson code. Some graph theory is also used in establishing what appears to be a new proof of the classical isomorphism, $A_8 \cong PSL(4,2)$. While this thesis

ffers new

pics in

e applic

des. In

ntersecti

nditions

s most he

esigns.

offers new definitions, proofs, or results for each of these topics in finite mathematics, the major contribution lies in the application of t-designs to the study of non-linear codes. In fact, it is the concept of the generalized block intersection numbers for t-designs, yielding necessary conditions for the building and extension of t-designs, which is most helpful in the analysis of non-linear codes and their designs.

THE UNIQUENESS OF THE NORDSTROM-ROBINSON AND THE GOLAY BINARY CODES

By

Stephen Lee Snover

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1973

DEDICATION

To my parents, without whose
stimulus I might not have gone so far,

and

To my loving wife, Ans, for her support.

ACKNOWLEDGMENTS

Many thanks go to

Professor J. J. Seidel for his fine teaching, good example, and patient guidance;

Professor J. M. Goethals for his stimulating discussions and above all for suggesting the topic of this thesis;

Professor L. M. Kelly for his thorough reading, suggested changes, and administrative assistance;

Professor W. Jonsson for suggestions on the structure of Chapters 9 and 11;

The Michigan State University Mathematics Department and the Technical University of Eindhoven Mathematics Department for their financial support;

Annerie 't Hart-Wustefeld and Sue Stewart for their fine typing.

TABLE OF CONTENTS

All

equation

out this

example,

in Secti

the chap

position

is disca

necessar

in the s

referred

originat

used. F

referred

same the

In

followi

Numbering and Notation

All the theorems, corollaries, lemmas, and important equations and remarks are numbered consecutively throughout this thesis with a three position label. For example, theorem (6.5.9) is the ninth item worth labelling in Section 5 of Chapter 6. If an item is referred to in the chapter in which the item originally appears, a two position reference number is given; the chapter number is discarded in this case because it is not really necessary and because then the fact that this item occurs in the same chapter will be emphasized. If an item is referred to in a different chapter from where it originates, the entire three position reference number is used. For example, within Chapter 6, Theorem (6.5.9) is referred to as Theorem (5.9), and in other chapters, the same theorem is referred to as Theorem (6.5.9).

In various places throughout this thesis the following notation shall be used:

$:=$	means "is defined to be" .
$\|X\|$	means the cardinality of set X .
$X \setminus Y$	means the set difference of X and Y, i.e. $X \setminus Y :=$ the set of elements in X but not Y .
$X \Delta Y$	means the symmetric difference of sets X and Y, i.e. $X \Delta Y := (X \setminus Y) \cup (Y \setminus X)$.

$\varphi \mid \mathcal{B}$	is the map φ with its domain restricted to the set $\mathcal{B}$.
S_n, A_n	mean the symmetric and alternating groups on n letters.
$PSL(n,2)$ $\overline{O}_6(+,2)$	are notations used for certain classical simple groups by E. Artin in [1] .

PART A: INTRODUCTION

CHAPTER 1

§1.1 Heuristic Introduction

In all forms of human communication messages are sent by means of codes. We naturally code our ideas into English phrases and sentences. English is a prototype for the kind of code we wish to discuss, as it is a code involving an agreed upon alphabet, a dictionary of code words which are meaningful sequences of letters from this alphabet, and messages being sentences or special sequences of words. We should note that not all sequences of letters form words, nor all sequences of words, messages.

Some codes, those commonly used during war times, are designed to disguise messages so that no one but the intended receiver can understand the message properly. Such codes are called minimum decodable. We will be concerned, however, with more common and very different types of codes -- maximum decodable or error correcting codes. These codes are designed to send messages in a way that even errors in transmission do not change or destroy the intended meaning of the message.

Errors in speaking or writing English, i.e. mispronunciations or misspellings, are most often detected

because
of lette
can then
the send
small ch
misunder

Err
followin

so that
of messa

number o
code word
practice
the end
than a t
(as in A
so-called

Tech
correctin
the alpha
of A be
is a subs

because the resulting "words" are meaningless sequences of letters (words that are not in the code). Such errors can then be corrected either from context or by asking the sender to repeat the message. Sometimes, however, small changes in spellings or pronunciations cause misunderstandings.

Error correcting codes are designed with the following desirable features:

(1) The alphabet is simple; there are few symbols.

(2) There are enough words to convey any message, so that it is not necessary to rely upon context or repeats of messages in order to correct transmissional errors:

(3) Words are not too "close" together, i.e. the number of letters that need to be changed to convert a code word into another is relatively large. Finally, in practice it is important to be able to distinguish between the end of one word and the beginning of the next by other than a time lapse (as in English) or a punctuation mark (as in Amharic, the Ethiopian language). Therefore, the so-called fixed block length codes require that

(4) Words all are of a fixed length of n letters.

Technically we may describe a fixed block length error correcting code as follows: Let $A := \{0,1,2,\ldots,k-1\}$ be the alphabet and $S :=$ the cartesian product of n copies of A be the code space. A code C in the code space S is a subset of S. Each element $\underline{x}$ in C is called a

"word" of C and $\underline{x} := (x_1, x_2, \ldots, x_n)$, where x_i is the i-th letter of the code word $\underline{x}$. A reasonable measure of distance between two words is the number of places in which their corresponding i-th letters differ. This is the historical definition of the "Hamming distance" between words.

A code C is often specified by the four parameters (k,n,M,d) where k is the cardinality of the alphabet, n is the length of each word, M is the number of code words in code C, and d is the minimum distance between any pair of code words from C. These parameters correspond directly to the four features of an error correcting code.

In this thesis, only the case of alphabets of two letters is considered. We therefore shorten the parameters for a code the (n,M,d) with $k = 2$ being understood.

Parameter d needs more explanation to make clear the correspondence between d and the ability to correct transmission errors in received words without relying upon context or repeats. In the example of English, the minimum distance is 1 since the words "step" and "stop" differ only in one place. If "step" is sent and "stop" received, you might not be able to even detect the error, let alone be able to correct it. If English were refined so that no two words in the dictionary differed by only

one letter, then the minimum distance would still be small, namely 2, as exhibited by the pair of words "sign" and "sing". In general we would like a code to have a relatively high minimum distance d so that such minor changes would not go unnoticed.

Although any subset of a code space S is a code, not every one is "good". Most codes with many words are like English in that the minimum distance between some pairs of words equals 1. "Good" codes have a maximum number of code words relative to their parameter values of n and d. Thus, a fundamental problem in coding theory is the determination of the largest possible code and its "structure" that can be selected in a given code space if the minimum distance between code words is specified.

In a way, the search for "good" codes amounts to a search for sphere packings in given code spaces. Because the Hamming distance is a legitimate distance function which satisfies the triangle inequality, the spheres of radius e about each code word in a (n,M,d) code are disjoint spheres, when $e = [(d-1)/2]$. Codes having the property that the spheres of radius e pack the code space are so "good" that they are called perfect. All perfect codes are known (for k being any prime power) and nearly-perfect and quasi-perfect codes are the topic of much current study.

If

power of

alphabet

vector s

$\underline{y} = (y_1,$

$\underline{x}+\underline{y} = ($

$\underline{xy} = (x_1$

being pe

immediate

imposed

about the

study of

Code

their co

about th

linear c

non-linea

this the

some non-

1.2 The

The

Even

or the No

history o

40], in

and 5-

If k (the number of letters in the alphabet) is a power of a prime, field properties may be imposed upon the alphabet so that the code space S has the structure of a vector space where, if $\underline{x} = (x_1, x_2, \ldots, x_n)$ and $\underline{y} = (y_1, y_2, \ldots, y_n)$ are any two vectors in S, then $\underline{x} + \underline{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$ and $\underline{xy} = (x_1y_1, x_2y_2, \ldots, x_ny_n)$, the component-wise operations being performed in $GF(k)$. These operations have no immediate intuitive interpretations, however, and are imposed merely in order to apply what is already known about the algebra and geometry of vector spaces to the study of codes.

Codes having the property that they are subspaces of their code vector space are called linear; more is known about this kind of code than any other. Unfortunately, linear codes are not in general as "good" as other non-linear codes. One of the major accomplishments of this thesis is the presentation of a new method of handling some non-linear, "good" codes.

§1.2 The History of the Fundamental Questions in this Thesis

Even before the discovery of either the Golay $(23, 2^{12}, 7)$ or the Nordstrom-Robinson $(15, 2^8, 5)$ binary codes, the history of their uniqueness began. In 1927 Witt [39] and [40], in an effort to establish the uniqueness of the 4- and 5- transitive Mathieu groups M_{23} and M_{24}

demo

5(4,

as a

disc

any

weig

line

weig

show

the

ther

binar

syste

and p

respe

Golay

in or

group

showe

would

bring

and t

uniqu

codes

demonstrated the uniqueness of the Steiner systems, $S(4,7,23)$ and $S(5,8,24)$, on which these groups operate as automorphism groups. Then shortly after Golay discovered his $(23,2^{12},7)$ code Paige [29] showed that any $(23,2^{12},7)$ code possesses a $S(4,7,23)$ as its set of weight 7 code vectors. Since Golay defined his code to be linear, Paige could then display 12 linearly independent weight 7 vectors in the $S(4,7,23)$, which was already shown to be unique by Witt, and claim that M_{23} is also the automorphism group of Golay's code.

Pless [31] reproduced Paige's arguments and extended them to showing that any linear $(23,2^{12},7)$ or $(24,2^{12},8)$ binary code contains $S(4,7,23)$ or $S(5,8,24)$ Steiner system as its set of non-zero minimal weight code vectors and possesses the automorphism group M_{23} or M_{24}, respectively. However, both Paige and Pless relied on Golay's original definition of the linearity of his code in order to establish the facts about the automorphism groups and uniqueness, in spite of the fact that they showed that an arbitrary code with the right parameters would contain the appropriate Steiner system. This brings up the following question:

Question #1: Is the uniqueness of the $S(4,7,23)$ and the $S(5,8,24)$ systems sufficient to imply the uniqueness of the $(23,2^{12},7)$ and $(24,2^{12},8)$ binary codes without the restriction of linearity?

If the answer be affirmative, then clearly by quoting Pless, Paige, and Witt, the unique codes of those parameters would also possess the automorphism groups, M_{23} and M_{24}.

Golay's codes have the maximum number of possible code vectors relative to their lengths and distances, a property also shared by Nordstrom and Robinson's $(15,2^8,5)$ and $(16,2^8,6)$ non-linear codes. When analyzing Golay's $(24,2^{12},8)$ code, J. M. Goethals [15] noticed that this code contained a $(16,2^8,6)$ non-linear code in a special way, and from this construction, he was able to find the automorphism group of this code. Although he never established a correspondence between Nordstrom-Robinson's $(16,2^8,6)$ code and his, Goethals was privately convinced that they were the same and that perhaps the code in question was unique. So it was Goethals who inspired the following:

Question #2: Are the $(15,2^8,5)$ and $(16,2^8,6)$ Nordstrom-Robinson codes unique?

Question #3: Are the automorphism groups of these codes A_7 and A_7 extended by the elementary abelian group of order 16, respectively?

Question #4: Does the $(16,2^8,6)$ code extend to the Golay $(24,2^{12},8)$ code in essentially one way?

These four questions are all answered affirmatively in this thesis. All the definitions, developments, and proofs to these questions are completely self-contained

her

[1.

thi

[15

[24

new

[23]

four

mini

Robi

desi

ques

equi

the

Weig

was

of t

the

it is

to th

defin

Gener

herein, and the results of all but Question #3 are new.

§1.3 The Scope of this Thesis

Although the basic and most difficult theorems in this thesis show the uniqueness of the Nordstrom-Robinson $(15,2^8,5)$ and $(16,2^8,6)$ and the Golay $(23,2^{12},7)$ and $(24,2^{12},8)$ binary codes, this is certainly not the only new nor important concept.

In a manner similar to Paige's analysis of the Golay $(23,2^{12},7)$ code [29], we proceed toward answering the four basic questions of the thesis by showing that the minimal weight non-zero code words in the Nordstrom-Robinson $(16,2^8,6)$ code form a t-design, a $4-(3,6,16)$ design with $d \geq 6$, which we call an XNR-design. Then the question of the uniqueness of this code is found to be equivalent to the uniqueness of the XNR-design. While the uniqueness of the $S(4,7,23)$ design of minimal weight non-zero code vectors in the Golay $(23,2^{12},7)$ code was proved to be unique by Witt even before the discovery of the code, neither the existence nor the uniqueness of the XNR-design seem to have previously been known. Thus it is, that t-designs become basic in the analysis leading to the uniqueness proofs of this thesis.

To the theory of t-designs, we unveil a new definition, t-designs with $d \geq d_0$, and a new tool, generalized block intersection numbers for any t-design.

The
one
use
The
Man
blo
ana
Fir
of
t-d
cod
can
Wit
cod
des
In
jus
ass

a ne
firs
desi
abe
at a
of t
esse

The extra condition, $d \geq d_0$, for any t-design enables one to distinguish among those t-designs which might be useful for binary coding theory purposes and the rest. The generalized block intersection numbers, a link between Mendelsohn's intersection numbers [25] and J. M. Goethal's block intersection numbers [16], become fundamental to the analysis, being essential in Chapters 5, 6, 7, 11, and 12. First of all, they are helpful in proving that the uniqueness of the codes is equivalent to the uniqueness of the t-designs of the minimal non-zero weight vectors of those codes. These numbers prove that the $S(5,8,24)$ design can be built in essentially one way from the XNR-design. With these numbers, we can deduce that any $(24,2^{12},8)$ code is necessarily the linear span of the $S(5,8,24)$ design formed by its minimal weight non-zero code vectors. In fact, these new generalized intersection numbers are just the tool necessary to tackle these codes without assuming any linearity.

Permutation groups come into play in order to establish a new construction of the important XNR-design, perhaps the first direct explicit construction. Constructing this design to contain the group A_7 extended by the elementary abelian group of order 16, it is then possible to conclude at a later time that this group is the automorphism group of the unique Nordstrom-Robinson code $(16,2^8,6)$ and its essential design.

we r

of

we e

isom

to t

appr

follo

11.4

Quest

and

uniqu

codes

Words

their

codes

In order to establish the uniqueness of the XNR-design, we need to appeal to the action of A_7 on the geometry of PG(3,2). Instead of quoting the literature, however, we establish what appears to be a new proof of the classical isomorphism $A_8 \cong PSL(4,2)$, and then restrict our attention to the action of A_7 .

This thesis attempts to present new results, new approaches, or at least new proofs in each of the following studies:

(1) coding theory
(2) t-designs
(3) automorphism groups
(4) finite vector spaces over GF(2), especially PG(3,2).

§1.4 The Organization Scheme of the Chapters

As explained in §1.2, this thesis answers the four questions:

Question #1: Is the uniqueness of the S(4,7,23) and S(5,8,24) Steiner systems sufficient to imply the uniqueness of the $(23,2^{12},7)$ and $(24,2^{12},8)$ binary codes without the restriction of linearity?

Question #2: Are the $(15,2^8,5)$ and $(16,2^8,6)$ Nordstrom-Robinson codes unique up to a permutation of their 15 and 16 coordinates, respectively?

Question #3: Are the automorphism groups of these codes A_7 and A_7 extended by the elementary abelian

group of order 16, respectively?

Question #4: Does the $(16,2^8,6)$ code extend to the Golay $(24,2^{12},8)$ code in essentially one way?

We shall now explain how the chapters of this thesis are organized in order to answer these questions.

First of all, the second through fifth chapters are introductory in nature, developing definitions, examples, and constructions of the codes under consideration. Definitions used in more than one of the following chapters are defined in these initial chapters. Other definitions, for example those concerning graph theory, occur within the only chapter where they are used. As often as possible, the examples used to explain the definitions are examples that will be referred to in a later part of this work. Also within these introductory chapters are constructions of the Golay codes, the S(4,7,23) and S(5,8,24) Steiner systems, the Nordstrom-Robinson codes and the XNR-design. Chapters 2 and 3 are devoted to coding theory definitions and the existence of the codes under study, Chapter 4 to t-designs and the development of the generalized block intersection numbers, and Chapter 5 to permutation groups and an explicit construction of the XNR-design.

Commencing with Chapter 6, we embark on an analysis of the Nordstrom-Robinson codes culminating, in Chapter 10, with the affirmative answers to Questions #2 and #3.

by tr

23,2

prope

Robin

a rax

and m

are a

non-z

C C

Quest

that

way (

lies

inter

weigh

neces

6 co

inter

reduc

NMR-d

of thi

genera

design

This analysis begins in the first half of Chapter 6 by trying to parallel Paige's analysis of Golay's $(23,2^{12},7)$ code. Although Golay's code is perfect, the property Paige made use of in his proofs, the Nordstrom-Robinson codes are not. However, both types of codes have a maximal number of code vectors relative to their length and minimum distance parameters. Using this property, we are able in Theorem (6.3.1) to show that the minimum weight non-zero code vectors of any $(16,2^{8},6)$ code, C, with $0 \in C$, form a XNR-design.

We find ourselves well on the way to answering Question 2 in the second half of Chapter 6 after proving that any XNR-design builds a $(16,2^{8},6)$ code in a unique way (Theorem (6.5.9)). The key to this important theorem lies in calculating and analyzing the generalized block intersection numbers for the XNR-design determined by the weight 6 vectors of the code. These numbers indicate necessary requirements for augmenting this set of 112 weight 6 code vectors to a $(16,2^{8},6)$ code. So thanks to these intersection numbers and the theorems of Chapter 6, we reduce the question of uniqueness to the study of the XNR-design.

In Chapters 7, 8, and 9 the question of the uniqueness of this XNR-design is answered. Chapter 7 employs the generalized intersection numbers to prove that any XNR-design is embeddable in a copy of $V(4,2)$, the finite four

dimensional vector space over GF(2), Theorem (7.5.1). In other words, the blocks of the XNR-design can be viewed as special subsets of points in PG(3,2), the projective space of 3 dimensions over GF(2). Chapter 8 occurs as an intermezzo, developing line coordinates (Theorem (8.10.1) for the lines of PG(3,2), which line coordinates are then used in Chapter 9 to prove the uniqueness of the design within the framework of the geometry of PG(3,2), Theorem (9.5.1).

Finally, Chapter 10 assembles the results of Chapters 6, 7, 8, and 9 to answer the fundamental Questions 2 and 3. Questions 1 and 4 relating to the Golay codes are considered in Chapters 11 and 12 after all the work relative to the XNR-design has been completed.

Since it was shown in Chapter 6 that the $(16,2^8,6)$ code is unique if and only if the XNR-design is also unique and since a similar theorem will be shown in Chapter 12 relative to the Golay $(24,2^{12},8)$ code and the S(5,8,24) design, Chapter 11 tackles Question 4 by considering only the designs in question. Chapter 11 shows that, up to an arbitrary permutation of the 7 additional coordinates, the XNR-design builds a S(4,7,23) in a unique way, Theorem (11.2.8). They by appling the fact that the S(5,28,24) design can be built from the S(4,7,23) design only by adding a new $24^{\underline{th}}$ coordinate which acts as a parity check on the other 23 coordinates, Theorem (11.3.9),

we have the theorem that the XNR-design builds S(5,8,24) in essentially one way. Use of the generalized block intersection numbers relative to each of the large Steiner systems is requisite in the proofs of this theorem. Inspired by the approach of Chapter 8, which was the real reason for including that chapter as it appears, we can establish the uniqueness of both the S(4,7,23) and the S(5,8,24) designs relative to the already proven uniqueness of the XNR-design. Furthermore, as a corollary to these uniqueness theorems, we can establish the facts that the automorphism groups of these Steiner systems are 4- and 5- transitive on the points of the designs, respectively, as well as block transitive on them, Theorems (11.2.18), (11.3.14), (11.2.16), and (11.3.13).

By almost literally duplicating the proof of theorem (6.5.9), but relative to the Golay $(24,2^{12},8)$ code and S(5,8,24), we can show in Theorem (12.3.5) that the $(24,2^{12},8)$ code is unique since the S(5,8,24) is unique. This proof uses the generalized block intersection numbers to full advantage and establishes the equivalence with no assumption of linearity. In fact, linearity of the unique $(24,2^{12},8)$ code is a lucky, non-essential outcome. Since we can answer Questions 4 and 1 affirmatively after proving Theorem (12.4.1), we now have reached the goal of these chapters.

car
n-d
ele
col
mat
in
cod
of
spa
ass

rela
near
with
The
also
this

PART B: PRELIMINARIES

CHAPTER 2

Binary Codes: Basic Definitions and Properties

§2.1 Introduction

A binary code will be viewed in this thesis as a carefully chosen subset of the set of all vectors of an n-dimensional vector space over GF(2), the field of two elements. We shall customarily write the code vectors as column vectors and represent the entire code by an incidence matrix whose columns are precisely all the code vectors. As in the case with the Nordstrom-Robinson and Golay binary codes, this incidence matrix can be considered as a collection of t-designs; and as such, the concepts of binary vector spaces, binary codes, t-designs, and automorphism groups assist one another.

This chapter includes most of the needed definitions relating to binary codes. The concepts of perfect and nearly perfect codes are defined in the next chapter along with definitions of the Golay and Nordstrom-Robinson codes. The tools relating to t-designs and automorphism groups will also come later. (References about binary coding related to this chapter are [3], [21], and [30].)

§2.2 Binary Vector Spaces

(2.1) Let $V(n,2)$ denote the vector space of n dimensions over $GF(2)$, the Galois Field of the two elements, 0 and 1. Let $\underline{x}$ denote any vector in $V(n,2)$. Sometimes elements of $V(n,2)$ shall be called points. Let $B := \{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$, be a basis of $V(n,2)$. Then relative to B, each $\underline{x} \in V(n,2)$ is uniquely represented as a column vector, $\underline{x} = (x_1, x_2, \ldots, x_n)^T$, where each $x_i \in GF(2)$ for $i = 1,2,\ldots,n$, and where ^{T} denotes the transpose of the indicated row vector. Unless otherwise stated, $V(n,2)$ will always be considered as possessing a given fixed basis. Let $\underline{0}$ and $\underline{1}$ be the vectors of $V(n,2)$ all of whose entries are either 0 or 1, respectively.

(2.2) Let $PG(n-1,2)$ denote the set of one-dimensional subspaces of $V(n,2)$. Since the equation

(2.3) $\underline{x} + \underline{y} = \underline{0}$ for $\underline{x}, \underline{y} \in V(n,2)$

is equivalent over $GF(2)$ to

(2.4) $\underline{x} = \underline{y}$,

it follows that $PG(n-1,2) = V(n,2) \setminus \{\underline{0}\}$.

Call a non-zero vector of $V(n,2)$ a point, when considered as an element of $PG(n-1,2)$.

The mapping

(2.5) $(\ , \ ) : V(n,2) \times V(n,2) \to GF(2)$

given by

$$(\underline{x}, \underline{y}) = \sum_{i=1}^{n} x_i y_i \quad \text{(modulo 2)}$$

for

$y =$

for

any

is

y

in-

For

is

$\underline{x}$

set

add

of

V,

lin

pre

Cor

the

dim

0-di

of

of

for the vectors $\underline{x} = (x_1, x_2, \ldots, x_n)^T \in V(n,2)$, $\underline{y} = (y_1, y_2, \ldots, y_n)^T \in V(n,2)$ defines a symmetric bilinear form, which is an inner product. For a given $\underline{x} \in V(n,2)$ any $\underline{y} \in V(n,2)$ such that

$$(\underline{x}, \underline{y}) = 0$$

is said to be <u>orthogonal</u> to $\underline{x}$ in $V(n,2)$. The set $\{\underline{y} \mid (\underline{x}, \underline{y}) = 0, \underline{y} \in V(n,2)\}$ for a given $\underline{x} \in V(n,2)$ is the $(n-1)$-dimensional subspace of $V(n,2)$ <u>orthogonal</u> to x. For a point $\underline{x} \in PG(n-1,2)$, the set $\{\underline{y} \mid (\underline{x}, \underline{y}) = 0, \underline{y} \in PG(n-1,2)\}$ is a <u>hyperplane</u> of $PG(n-1,2)$ and is called the <u>polar</u> of $\underline{x}$ in $PG(n-1,2)$.

(<u>Linear</u>) subspaces of $PG(n-1,2)$ are (perhaps empty) sets of points of $PG(n-1,2)$ which are closed under vector addition defined in $V(n,2)$. It is well known that the set of all subspaces of $PG(n-1,2)$ forms a lattice under $\wedge$ and $\vee$, which are given respectively by set intersection and linear span. <u>Collineations</u> of $PG(n-1,2)$ are lattice preserving permutations of the points of $PG(n-1,2)$. <u>Correlations</u> are lattice inverting permutations, which send the i-dimensional subspaces of $PG(n-1,2)$ to $((n-1)-i)$ dimensional supspaces, for $-1 \leq i \leq n-1$ where points are 0-dimensional supspaces and $\emptyset$ the (-1)-dimensional subspace of $PG(n-1,2)$. In particular, correlations exchange the sets of points and hyperplanes of $PG(n-1,2)$.

§2.3 Binary Codes

Given any two vectors $\underline{x} = (x_1, x_2, \ldots, x_n) \in V(n,2)$ and $\underline{y} = (y_1, y_2, \ldots, y_n) \in V(n,2)$, with coordinates relative to a given fixed basis of $V(n,2)$, then define the following:

The weight, $|x|$, of a vector $\underline{x} \in V(n,2)$ is a mapping $|\ |: V(n,2) \to$ the set of integers, $\mathbf{Z}$ given by

(3.1) $|x| := \sum_{i=1}^{n} x_i$, where addition is now computed in $\mathbf{Z}$.

The (Hamming) distance *, $d(\underline{x},\underline{y})$, between two vectors, $\underline{x}$ and $\underline{y} \in V(n,2)$ is

(3.2) $d(\underline{x},\underline{y}) := |\underline{x} + \underline{y}|$.

The coordinate-wise product of two vectors is

(3.3) $\underline{xy} := (x_1y_1, x_2y_2, \ldots, x_ny_n)$.

A vector $\underline{x}$ is contained in a vector y,

(3.4) $\underline{x} \leq \underline{y}$ iff $\underline{x} = \underline{xy}$.

One can easily check the following list of properties that pertain to the above definitions:

(3.5) the Hamming distance is a distance function.

(3.6) $|\underline{x}| + |\underline{y}| = |\underline{x} + \underline{y}| + 2|\underline{xy}|$.

(3.7) $\underline{xx} = \underline{x}$.

(3.8) $\leq$ is a partial ordering on vectors of $V(n,2)$.

(3.9) $\underline{x} \leq \underline{y}$ iff $|\underline{x} + \underline{y}| = |\underline{y}| - |\underline{x}|$.

---

*The Hamming distance is the square of the customary Euclidean distance in the binary case.

A (binary) code, C, is any set of vectors from $V(n,2)$.

(3.10) A code word is a vector $v \in V(n,2)$ that is also in C. A (n,M,d_0) code C is a code C of $|C| = M$ vectors from $V(n,2)$ so that

(3.11) $$\min_{\substack{x,y\in C \\ x\neq y}} |\underline{x} + \underline{y}| \geq d_0 .$$

(3.12) We sometimes write "C is a code with $d \geq d_0$" or "C has minimum distance d_0" if C is an (n,M,d_0) code and if the value of n is understood.

(3.13) A linear code C is a code satisfying

$$\underline{x},\underline{y} \in C \text{ imply } \underline{x} + \underline{y} \in C .$$

(3.14) A linear code is a subspace $V(m,2)$ of $V(n,2)$ for $0 \leq m \leq n$, and is said to have dimension m. Any linear code C with at least one code word contains $\underline{0}$, and as such is an $(n,2^n,d_0)$ code for

(3.15) $$d_0 = \min_{\substack{x\in C \\ x\neq 0}} |\underline{x}| .$$

We shall, for the most part, consider non-linear codes, although occasionally the concept of linear codes is a useful tool in this thesis.

§2.4 Incidence Matrices

(4.1) An incidence matrix for an (n,M,d_0) code C is an $n \times M$ zero-one matrix whose columns are the code words (per def. (3.10))

(4.2) If C is a linear code, then one may choose a basis of code words and form an $n \times m$ matrix $\underline{G}$ called a <u>generator matrix</u> for C, having as columns those m basis vectors which span the code (a $V(m,2)$ subspace, cf. (3.14)). Let C be a code, and define

(4.3) $C^{\perp} := \{\underline{y} \in V(n,2) \mid (\underline{x},\underline{y}) = 0 \text{ for all } \underline{x} \in C\}$.

$C^{\perp}$ is called the <u>code orthogonal</u> to C.

By the definition (4.3) of $C^{\perp}$ it is clear that the following properties hold:

(4.4) $C^{\perp}$ is always a linear code.

(4.5) $(C^{\perp})^{\perp}$ is the linear span of C.

(4.6) $(C^{\perp})^{\perp} = C$ iff C is linear.

(4,7) Let any generator matrix of $C^{\perp}$ be denoted by H and be called a <u>parity check matrix of C</u>.

We now proceed to define the Hamming codes in terms of the generator matrix of their orthogonal codes. Let H_n be the $(2^n-1) \times n$ matrix whose rows are all the (2^n-1) distinct non-zero vectors of $V(n,2)$, and so placed in H_n, that the $i^{\underline{th}}$ row of H_n represents (relative to a fixed basis of $V(n,2)$) the binary expansion of the integer i, for $1 \leq i \leq 2^n-1$. Let

(4.8) $C_n := \{\underline{x} \in V(2^n-1,2) \mid \underline{x}^T H_n = \underline{0}^T\}$.

The code C_n is called the <u>Hamming code</u> of length 2^n-1.

(4.9) <u>Lemma</u>: C_n is a linear $(2^n-1, 2^{(2^n-1-n)}, 3)$ code.

<u>Proof</u>:

Property (4.5) shows that C_n is linear. Then it is

cle

che

the

Q €

$\underline{x}^T H$

Wh

and

'2.5

code

of t

(5.1

Note

but

(5.2

matri

rows

(5.3

incid

extra

chose

are a

coord

(5.4)

clear that $|C_n| = 2^{((2^n-1)-n)}$. It now suffices to check $d_0 \geq 3$ in (3.15). If $|x| = 1$ for $x \in C_n$, then $\underline{x}^T H_n = \underline{0}^T$ implies that one of the rows of H_n is the $\underline{0} \in V(n,2)$, contradiction. If $|\underline{x}| = 2$, for $\underline{x} \in C_n$, then $\underline{x}^T H_n = \underline{0}^T$ implies that two distinct non-zero vectors of $V(n,2)$ are linearly dependent, contradicting equations (2.3) and (2.4). Hence, $d_0 \geq 3$. //

§2.5 Modifications of codes

Given an (n,M,d_0) code C , one can obtain related codes by a number of different standard modifications. Some of these are given in the following list of definitions.

(5.1) A coset, $C + \underline{x}$, of a code C is

$$C + \underline{x} := \{\underline{y} + \underline{x} \mid x \in V(n,2),\ \underline{y} \in C\} .$$

Note that if C is linear then $\underline{y},\underline{z} \in C + \underline{x}$ imply $y + z \in C$, but not so if C is not linear.

(5.2) A punctured code of C is a code with an incidence matrix identical with that for C except that one of the rows is eliminated.

(5.3) A parity check code of C is a code with an incidence matrix identical with that for C and with one extra row; the zero or one entries in the extra row are chosen so that the weights of the resulting column vectors are always even. The added row is called the parity check coordinate row.

(5.4) An equivalent code to code C is a code whose

incidence matrix N can be transformed into that for C after a suitable permutation of the rows and columns of N.

One can easily see that the following properties hold for a given (n,M,d_0) code C.

(5.5) A punctured code of C is a $(n-1,M,d_0-1)$ code.

(5.6) If d_0 is odd, then a parity check code of C is a $(n+1,M,d_0+1)$ code.

(5.7) The relation of "being an equivalent code" is an equivalence relation.

(5.8) A punctured code of a linear code C is again a linear code.

(5.9) A parity check code of a linear code C is again a linear code.

(5.10) As examples of parity check codes, we define the Extended Hamming code, $\overline{C_n}$, of length 2^n as the parity check code of C whose parity check coordinate row is the first row of the corresponding incidence matrix. Then by (5.6) and (5.9) we have proved:

(5.11) Lemma: The Extended Hamming code, $\overline{C_n}$, of length 2^n is a $(2^n, 2^{2^n-1-n}, 4)$ linear code.

§2.6 Geometric Codes

Let φ be any fixed one to one correspondence:

(6.1) $\varphi : V(2^n,2) \to 2^{V(n,2)}$

so that the standard basis vectors from a fixed basis B of $V(2^n,2)$ are mapped to points of $V(n,2)$. Then the vectors of $V(2^n,2)$ are called characteristic functions

of

(6.

so

exp

tha

(6.

base

the

char

PG'r

be i

PG(n

From

geom

in t

Theo

uniq

Nord

of subsets of the points of $V(n,2)$ relative to φ and B.

(6.2) Let $\varphi : \underline{e_i} \in B \to \underline{x} \in V(n,2)$ so that, relative to a fixed basis A of $V(n,2)$, the binary expansion of i is $\underline{x}$. From (6.2) it follows directly that:

(6.3) Lemma: For φ defined in (6.2) and for fixed bases A and B of $V(n,2)$ and $V(2^n,2)$ respectively, the code words in the Hamming code C_n, are precisely the characteristic functions of binary dependent sets from $PG(n-1,2)$.

A geometric code is a binary code, whose code words can be interpreted in terms of the geometries of $V(n,2)$ or $PG(n-1,2)$ by an appropriate one to one correspondence φ. From Lemma (6.3) one can see that the Hamming codes are geometric codes.

The Nordstrom-Robinson code, which will be defined in the following chapter, is also a geometric code, Theorem (7.5.1). This observation is a key step in the uniqueness proofs, Theorems (10.3.2) and (10.2.1), of the Nordstrom-Robinson code and its extension.

CHAPTER 3

Definitions and Existence of the Golay and Nordstrom-Robinson Binary Codes

§3.1 Introduction

The definitions and existence of the Golay and Nordstrom-Robinson codes will be presented in Sections 3.3 and 3.5. To this end it will be useful to establish the sphere packing bound, in Section 3.2, which gives an upper bound for the number, M, of code words in an $(n, M, (2e+1))$ code. Those codes satisfying equality in this bound are called perfect codes. Thus if C is a perfect code in $V(n,2)$ all the points of $V(n,2)$ can be "perfectly" covered by the disjoint spheres of (Hamming) radius e centered about the points of C. The Golay code is an example of a perfect code. The Nordstrom-Robinson code is not perfect, but does satisfy equality for a refinement of the sphere packing bound, called the specialized Johnson bound. This is introduced in Section 3.4. Codes satisfying equality in this bound are called nearly perfect codes, a name coined by Goethals and Snover [17]. The class of nearly perfect codes contains the class of perfect codes. In terms of $V(n,2)$, if C is a nearly perfect code, then the spheres of radius $e+1$ centered about points of C cover all points of $V(n,2)$. (The spheres are not disjoint in this

cas

Th

the

(1

cod

(2

(3

n =

iso

in

of

res

the

k_

sho

iso

the

uni

acc

to

is

Prep

case, though.)

All perfect codes are known. VanLint [21] and Tietäväinen and Perko [34] have shown that they must be of the following types:

(1) the Hamming (linear) codes and the Vasil'ev (non-linear) codes, both with parameters $(2^k-1, 2^{2^k-k-1}, 3)$ for any k,

(2) the Golay binary code with parameters $(23, 2^{12}, 7)$, and

(3) the trivial one word and two word codes of lengths $n = e$ and $n = e+1$ respectively for any e.

It is known that the Hamming codes are unique up to isomorphism. While no proof of this can readily be found in the literature, a proof similar to that of Theorem (7.4.4) of this thesis can be constructed. However, without the restriction of linearity, codes with the same parameters as the Hamming codes, $(2^k-1,\ 2^{2^k-k-1}, 3)$, are not unique for $k \geq 4$ as was shown by Vasil'ev [36]. In 1968 V. Pless showed [31] that any linear $(23, 2^{12}, 7)$ code must be isomorphic to the Golay code. One major purpose of this thesis is to establish the fact that the Golay binary code is unique even without the linearity assumption. This will be accomplished in Chapter 12.

Furthermore, the Nordstrom-Robinson code will be shown to be unique up to isomorphism in Chapter 10. This code is the first code in each of the infinite families of Preparata codes of parameters $(4^k-1,\ 2^{4^k-1-4k}, 5)$ for

k_2
(4^k-1

conce
the e
and t
the G

3.2

(2.1)

Then
C .
spher
as fo
(2.2)
Since
it sa
spher
code
follo

and g
(2.3)

$k \geq 2$ [32], and Kerdok codes of parameters $(4^k-1,\ 2^{4k},\ ((4^k-2^k)/2-1))$ for $k \geq 2$ [20].

Our present purpose in this chapter is to develop the concepts of perfect and nearly perfect codes, to establish the existence of the Golay and Nordstrom-Robinson codes, and to show that these codes are both nearly perfect while the Golay code is perfect.

§3.2 Perfect Codes

For a given (n,M,d_0) code C let

$$(2.1) \qquad e := \frac{d_0 - 1}{2} \quad .$$

Then e is called the error correcting capability of code C. C is said to be an e-error correcting code. Let the sphere, $B(\underline{w},r)$, of radius r about $\underline{w} \in V(n,2)$ be defined as follows:

$$(2.2) \qquad B(\underline{w},r) := \{\underline{y} \in V(n,2) \mid d(\underline{w},\underline{y}) \leq r\} \ .$$

Since the Hamming distance is a distance function by (2.3.5), it satisfies the triangle inequality. Therefore, the spheres of radius e about code words in the given (n,M,d_0) code C must be disjoint. This observation proves the following inequality:

$$\Big| \bigcup_{\underline{x} \in C} B(\underline{x},e) \Big| \leq |V(n,2)| = 2^n \ ,$$

and gives the sphere packing bound:

$$(2.3) \qquad |C| \cdot \left(1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{e}\right) \leq 2^n \ .$$

(2.4

pack

e =

|C|

cons

nece

(2.1

(2.5

perf

Proo

(3.3

H. F

$\overline{C_3}$,

code

(23,

this

inci

indi

form

are

(2.4) A code C satisfying equality in the sphere packing bound (2.3) is called a perfect code. Notice that $e = n$ yields the trivial solution of equality in (2.3) for $|C| = 1$; the corresponding code C is the trivial code, consisting of (any) one vector of $V(n,2)$. For $|C| > 1$, necessarily $e < n/2$, in which case e is defined as in (2.1).

(2.5) Lemma: The Hamming code C_n of length 2^n-1 is perfect.

Proof: $2^{(2^n-1)-n)} \cdot (1 + (2^n-1)) = 2^{2^n-1}$. //

§3.3 Definition of the Golay Code

With a construction method due to E. F. Assmus and H. F. Mattson, cf. VanLint [21], we shall construct from $\overline{C_3}$, the extended Hamming code of length 8, a $(24,2^{12},8)$ code. Then by puncturing this code we shall show that the $(23,2^{12},7)$ code called the Golay binary code obtained in this way is linear and perfect with $e = 3$.

Let $\overline{C_3}$ be the extended Hamming code of length 8 with incidence matrix N given in Figure (3.1). Notice that the indicated 7×7 submatrix M is the familiar symmetric form of the incidence matrix of $PG(2,2)$. The rows of N are numbered by φ (cf. (2.6.1) with the integers $0,1,2,\ldots,7$.

Figure (3.1)

		N														
0	0 0 0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0
1	0 0 1	0	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1
2	0 1 0	0	0	0	1	1	0	1	0	1	1	1	0	0	1	0	1
4	1 0 0	0	0	0	0	1	1	0	1	1	1	1	1	0	0	1	0
5	1 0 1	0	1	0	0	0	1	1	0	1	0	1	1	1	0	0	1
7	1 1 1	0	0	1	0	0	0	1	1	1	1	0	1	1	1	0	0
3	0 1 1	0	1	0	1	0	0	0	1	1	0	1	0	1	1	1	0
6	1 1 0	0	1	1	0	1	0	0	0	1	0	0	1	0	1	1	1
				M													

Figure (3.2)

0	0 0 0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0
6	1 1 0	0	1	1	0	1	0	0	0	1	0	0	1	0	1	1	1
3	0 1 1	0	1	0	1	0	0	0	1	1	0	1	0	1	1	1	0
7	1 1 1	0	0	1	0	0	0	1	1	1	1	0	1	1	1	0	0
5	1 0 1	0	1	0	0	0	1	1	0	1	0	1	1	1	0	0	1
4	1 0 0	0	0	0	0	1	1	0	1	1	1	1	1	0	0	1	0
2	0 1 0	0	0	0	1	1	0	1	0	1	1	1	0	0	1	0	1
1	0 0 1	0	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1

Perform the row permutation (16)(23)(47) on N , inverting the order of the last seven rows, and obtain the equivalent code $\overline{C_3'}$, (cf. figure (3.2)) and N'

(3.3) Claim: (1.) $\overline{C_3} \cap \overline{C_3'} = \{\underline{0}, \underline{1}\}$.

(2.) All code words of $\overline{C_3}$ and $\overline{C_3'}$ have weights 0, 4, and 8 .

(3.) All vectors of the form $\underline{x} + \underline{y}$, where $\underline{x} \in \overline{C_3}$ and $\underline{y} \in \overline{C_3'}$ have even weight.

Proofs: Claims (1.) and (2.) are immediate from inspecting

the

in F

(2.

(3.4

Now

(3.5

$\underline{x} \in \overline{C}$

(3.6

Proo

That

the

form

that

least

(3.3)

(3.7)

If no

$|\underline{x}| =$

Since

$|\underline{a} + \underline{b}$

then

the incidence matrices N and N' of $\overline{C_3}$ and $\overline{C_3'}$ given in Figures 1 and 2 respectively. Claim (3.) follows from (2.) and Formula (2.3.6) which reads:

(3.4) $|x| + |y| = |\underline{x} + \underline{y}| + 2|xy|$.

Now define

(3.5) XGOLAY := $\{(\underline{a} + \underline{x}, \underline{b} + \underline{x}, \underline{a} + \underline{b} + \underline{x})^T \mid \underline{a},\underline{b} \in \overline{C_3}$ and $\underline{x} \in \overline{C_3'}\}$, to be the <u>extended Golay code</u>, or <u>XGOLAY</u>.

(3.6) <u>Theorem</u>: XGOLAY is a $(24, 2^{12}, 8)$ linear code.

<u>Proof</u>: That XGOLAY is linear is immediate from Definition 3.5). That XGOLAY has dimension 12 is an immediate consequence of the fact that $\underline{0}^T$ has no nontrivial representation of the form $(\underline{a} + \underline{x}, \underline{b} + \underline{x}, \underline{a} + \underline{b} + \underline{x})^T$. It now suffices to show that $d_0 \geq 8$.

If $\underline{v}^T = (\underline{a} + \underline{x}, \underline{b} + \underline{x}, \underline{a} + \underline{b} + \underline{x})^T \neq \underline{0}^T$ and if at least one of $\underline{a}$, $\underline{b}$, $\underline{a} + \underline{b}$, or $\underline{x}$ is either $\underline{0}$ or $\underline{1}$, then (3.3) implies that $|\underline{v}| \geq 8$.

Three applications of (3.4) yield the following equality:

(3.7) $$\begin{aligned} |\underline{a} + \underline{x}| + |\underline{b} + \underline{x}| + |\underline{a} + \underline{b} + \underline{x}| &= \\ &= |\underline{a} + \underline{b}| + 2|(\underline{a} + \underline{x})(\underline{b} + \underline{x})| + |\underline{a} + \underline{b} + \underline{x}| \\ &= |\underline{x}| + 2\{|(\underline{a} + \underline{x})(\underline{b} + \underline{x})| + (\underline{a} + \underline{b})(\underline{1} + \underline{x})|\} \\ &= |\underline{x}| + 2|\underline{a} + \underline{b} + \underline{ab} + \underline{x}| . \end{aligned}$$

If none of $\underline{a}$, $\underline{b}$, $\underline{a} + \underline{b}$, $\underline{x}$ are either $\underline{0}$ or $\underline{1}$, then $|\underline{x}| = 4$, and it is necessary to show $|\underline{a} + \underline{b} + \underline{ab} + \underline{x}| \geq 2$. Since $|\underline{a}| = |\underline{b}| = 4$ and (3.4) implies that $|\underline{ab}|$ is even, $|\underline{a} + \underline{b} + \underline{ab} + \underline{x}|$ must also be even. If $|\underline{a} + \underline{b} + \underline{ab} + \underline{x}| = 0$, then $\underline{a} + \underline{b} + \underline{ab} = \underline{x}$. Then $(\underline{a} + \underline{1})(\underline{b} + \underline{1}) = (\underline{x} + \underline{1})$, and

hence

[x] =

(3.8

code

(3.9

Proof

(3.10

(23,2

Proof

(3.4

d_0 =

(4.1)

parti

accor

for s

(4.2)

(4.3)

(4.4)

Proof

By th

* Late

equiva

hence $\underline{a} = \underline{b} = \underline{x}$. Therefore $\underline{x} \in \overline{C_3} \cap \overline{C_3'}$, contradicting $|\underline{x}| = 4$. //

(3.8) Any punctured code of XGOLAY is called the * Golay code or GOLAY.

(3.9) Lemma: The Golay code is a linear $(23, 2^{12}, 7)$ code.

Proof: Use (2.5.5), (2.5.8), and Theorem (3.6). //

(3.10) Theorem: The Golay code is a perfect linear $(23, 2^{12}, 7)$ code.

Proof: $2^{12}(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}) = 2^{23}$. //

§3.4 Nearly Perfect Codes

Let C be any (n, M, d_0) code where $d_0 = 2e + 1$, i.e. d_0 is odd.

Let $B(\underline{w}, r)$ be as in (2.2) and $\underline{x} \in C$. Let

(4.1) $T(x) := \{\underline{v} \in V(n,2) \mid d(\underline{x}, \underline{v}) = e + 1\}$. Now partition $T(\underline{x})$ into two classes, $T_\alpha(\underline{x})$ and $T_\beta(x)$, according as the elements of $T(\underline{x})$ belong to some $B(\underline{y}, e)$ for some $\underline{y} \in C$, or not, that is,

(4.2) $T_\alpha(\underline{x}) := \{\underline{v} \in T(\underline{x}) \mid \exists\, \underline{y} \in C,\ \underline{v} \in B(\underline{y}, e)\}$.

(4.3) $T_\beta(\underline{x}) := \{\underline{v} \in T(\underline{x}) \mid \nexists\, \underline{y} \in C,\ \underline{v} \in B(\underline{y}, e)\}$.

(4.4) Lemma: For each $\underline{x} \in C$, $|T_\alpha(\underline{x})| \leq [(n-e)/(e+1)]\binom{n}{e}$.

Proof: Let $\underline{v} \in T_\alpha(\underline{x}) = e+1$, $d(\underline{v}, \underline{y}) \leq e$, $d(\underline{x}, \underline{y}) \geq 2e+1 = d_0$. By the triangle inequality, necessarily it follows that

$$d(\underline{v}, \underline{y}) + d(\underline{v}, \underline{x}) = d(\underline{y}, \underline{x}) = 2e+1 = d_0 .$$

---

*Later we shall prove that this code is unique up to equivalence, and so the article "the" is not a mistake.

In th

from

(4.5)

where

2e+1

least

place

coord

[(n-e

n el

cardi

(4.6)

Inequ

(4.7)

Proof

since

spher

S. Joh

number

terms

(4.8)

In this case

$$|T_\alpha(\underline{x}) \cap B(\underline{y},e)| = \binom{2e+1}{e+1},$$

from which,

(4.5) $$|T_\alpha(\underline{x})| = \binom{2e+1}{e+1} |N_{2e+1}(\underline{x})| ,$$

where $N_{2e+1}(\underline{x})$ is the set of code words $\underline{y}$ at distance $2e+1$ from $\underline{x}$. Since any two vectors in $N_{2e+1}(\underline{x})$ are at least a distance $2e+1$ apart, the $(2e+1)$-sets of coordinate places in which they both differ from $\underline{y}$ share at most t coordinate places. Furthermore since there are at most $[(n-e)/(e+1)]$ subsets of cardinality $(2e+1)$ of a set of n elements which share precisely a given subset of cardinality e, we deduce

(4.6) $$|N_{2e+1}(\underline{x})| \leq [(n-e)/(e+1)] \binom{n}{e} / \binom{2e+1}{e+1}.$$

Inequality (4.6) converts (4.5) into the desired result. //

(4.7) Corollary: $$|T_\beta(\underline{x})| \geq \binom{n}{e+1} - [(n-e)/(e+1)] \binom{n}{e} .$$

Proof: This result follows immediately from Lemma (4.4), since for any $\underline{x} \in C$,

$$|T_\alpha(\underline{x})| + |T_\beta(\underline{x})| = |T(\underline{x})| = \binom{n}{e+1}. \text{ //}$$

Now we are able to state and prove a refinement of the sphere packing bound, which is a specialized version of the S. Johnson bound [18]. The Johnson bound itself uses the numbers $\max_{\underline{x} \in C} |N_d(\underline{x})|$ rather than the particular value in terms of n and e given by inequality (4.6).

(4.8) Theorem: (the specialized Johnson bound)

For

equi

(4.9

whic

beca

Proo

V(n,

of t

$T_{\pm}(x$

leas

we c

(4.1

from

vect

2^n

(4.1

Near

of n

(4.1

code

For any code of length n, and minimum distance $2e+1$,

$$|C| \cdot \left(1 + \binom{n}{1} + \binom{n}{2} + \ldots + \frac{1}{[n/(e+1)]}\binom{n}{e}\left(\frac{n-e}{e+1} - \left\lfloor \frac{n-e}{e+1} \right\rfloor\right)\right) \leq 2^n .$$

Before proving this theorem we note the following equivalent form of the specialized Johnson bound:

$$(4.9) \quad |C| \cdot \left(1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{e-1} + \frac{1}{[(n+1)/(e+1)]}\binom{n+1}{e+1}\right) \leq 2^n$$

which is equivalent to that in the statement of Theorem (4.8) because

$$\left(\frac{n-e}{e+1} - \left\lfloor \frac{n-e}{e+1} \right\rfloor\right) = 0 \Leftrightarrow n \equiv -1 \pmod{e+1} \Leftrightarrow \left\lfloor \frac{n}{e+1} \right\rfloor \neq \left\lfloor \frac{n+1}{e+1} \right\rfloor .$$

Proof of Theorem (4.8):

There are at least $\left| \bigcup_{\underline{x} \in C} T_\beta(\underline{x}) \right|$ vectors of the space, $V(n,2)$, not contained in any $B(\underline{x},e)$, $\underline{x} \in C$. A given vector of the space can belong to at most $[n/(e+1)]$ distinct sets $T_\beta(\underline{x})$, for $\underline{x} \in C$, since vectors of the code are at least a distance $2e+1$ apart. Hence, using Corollary (4.7), we obtain

$$(4.10) \quad \left| \bigcup_{x \in C} T_\beta(\underline{x}) \right| \geq \frac{|C|}{[n/(e+1)]} \left(\binom{n}{e+1} - \left\lfloor \frac{n-e}{e+1} \right\rfloor \binom{n}{e}\right) ,$$

from which the result follows by noting that the number of vectors in $\bigcup_{\underline{x} \in C} (B(\underline{x},e) \cup T_\beta(\underline{x}))$ is less than or equal to 2^n .//

(4.11) Codes meeting the bound of Theorem (4.8) are called nearly perfect.

The next lemma shows the important fact that the class of nearly perfect codes contains the class of perfect codes.

(4.12) Lemma: Every perfect code is also a nearly perfect code.

Proof: The specialized Johnson bound reduces to the sphere packing bound exactly when $n+1 \equiv 0 \pmod{(e+1)}$. //

We can describe nearly perfect codes in more detail with:

(4.13) Lemma: For any nearly perfect e-error correcting code of length n

(i) any vector at a distance greater than e from every code word is at a distance e+1 from exactly $[n/(e+1)]$ code words,

(ii) any vector at a distance e from a given code word is at a distance e+1 from exactly $[(n-e)/(e+1)]$ other code words.

Proof: Equality in (4.9) implies equality also in (4.10) and (4.7). Equality in both (4.7) and (4.10) implies that each vector at a distance greater than e from each code word is at a distance e+1 from exactly $[n/(e+1)]$ code words, i.e. part (i). Equality in (4.7) together with (4.5) proves (ii).//

§3.5 Definition of the Nordstrom-Robinson Code

Various people involved in binary coding theory were aware in the early 60's that there might exist a (16,256,6) code. The specialized Johnson bound (Theorem (4.8)), which was known then, inspired the search, since this showed that no (16,M,6) code could have an $M > 256$. Moreover, since 256 is a power of 2, it was natural to ask if there was a linear code with parameters (16,256,6). Calabi et al.,

answe

[27]

that,

large

stude

and h

[28].

Robin

lengt

given

B. G.

2n f

linea

prove

abeli

V(n,2

theor

Furthe

$2^n/2^k$

Theref

(5.1)

$L = \{$

answered this question [7] in the negative. However, Nadler [27] had discovered in 1962 a (13,32,6) non-linear code, that, even up to today, is the (13,M,6) code with the largest known M value. Nordstrom and a high school student named Robinson were able to construct a (15,256,5) and hence a (16,256,6) non-linear code from Nadler's code [28].

In this section we construct the extended Nordstrom-Robinson code from $\overline{C_3}$, the extended Hamming code of length 8, in a way resembling the construction of XGOLAY given in Section 3.3. In this construction, due to C. L. Liu, B. G. Ong, and G. R. Ruth [22], we create a code of length 2n from two codes of length n, the first of which must be linear. In order to better understand this scheme, we first prove a few remarks and lemmas regarding linear codes.

Since a linear code C is a subgroup of the additive abelian group $\{V(n,2), +\}$, where + is vector addition in V(n,2), it is necessary (by the Lagrange theorem for group theory) that

$$|C| = M = 2^k \quad \text{for some} \quad 0 \leq k \leq n .$$

Furthermore, the set V(n,2) may be partitioned into $2^n/2^k = 2^{n-k}$ cosets (cf. Definition (2.5.1)) by C. Therefore,

(5.1) Lemma: Let C be a linear $(n,2^k,d)$ code and let $L = \{\ell_1, \ell_2, \ldots, \ell_{2^{n-k}}\}$ be a set of distinct coset

representatives, one chosen from each of the 2^{n-k} distinct cosets of C in $V(n,2)$. Then each $\underline{v} \in V(n,2)$ can be expressed uniquely as $\underline{v} = \underline{\ell} + \underline{m}$, where $\underline{\ell} \in L$ and $\underline{m} \in C$. We omit the standard proof.

Note that it is always possible to choose coset representatives $\underline{\ell}$ of minimum weight, since each coset $C + \underline{\ell}$ of C in $V(n,2)$ is a finite set.

Let $\overline{C_3}$ be the extended Hamming code of length 8. By Lemma (2.5.11), $\overline{C_3}$ is a linear (8,16,4) code and is given by the 8×16 incidence matrix of Figure (3.1). Let L be the set of 16 minimum weight coset leaders of $\overline{C_3}$ to cosets of $\overline{C_3}$ in $V(8,2)$ given in Figure (5.3).

Figure (5.3)

Cosets of $\overline{C_3}$ (identified by their leaders)	Assignment by f of words in $\overline{C_3}$ to the cosets
$\ell_i \in L$	$f(\ell_i) \in \overline{C_3}$
0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0	1 0 0 0 1 0 1 1
0 0 1 0 0 0 0 0	1 1 0 0 0 1 0 1
0 0 0 1 0 0 0 0	1 1 1 0 0 0 1 0
0 0 0 0 1 0 0 0	1 0 1 1 0 0 0 1
0 0 0 0 0 1 0 0	1 1 0 1 1 0 0 0
0 0 0 0 0 0 1 0	1 0 1 0 1 1 0 0
0 0 0 0 0 0 0 1	1 0 0 1 0 1 1 0
1 0 0 0 0 0 0 0	1 1 1 1 1 1 1 1
1 1 0 0 0 0 0 0	0 1 1 1 0 1 0 0
1 0 1 0 0 0 0 0	0 0 1 1 1 0 1 0
1 0 0 1 0 0 0 0	0 0 0 1 1 1 0 1
1 0 0 0 1 0 0 0	0 1 0 0 1 1 1 0
1 0 0 0 0 1 0 0	0 0 1 0 0 1 1 1
1 0 0 0 0 0 1 0	0 1 0 1 0 0 1 1
1 0 0 0 0 0 0 1	0 1 1 0 1 0 0 1

N^T where N is from Figure (3.1)

Now define

(5.4) XNR := $\{(\underline{v},\ \underline{v} + f(\underline{v}))^T \mid \underline{v} \in V(8,2)$ and $f(\underline{v}) = f(\ell_i + \underline{m}) = f(\ell_i)$ for f given in Figure (5.3)$\}$

to be the extended Nordstrom-Robinson code or XNR.

(5.5) Theorem: XNR is a $(16, 2^8, 6)$ code.

Proof: From (3.4) we may derive

$$(5.6)\quad |\underline{x} + \underline{y}| + |\underline{x} + \underline{y} + \underline{z}| = |\underline{z}| + 2|(\underline{x} + \underline{y})(\underline{x} + \underline{y} + \underline{z})|$$
$$= |\underline{z}| + 2|(\underline{x} + \underline{y}) + (\underline{x} + \underline{y})\underline{z}|$$
$$= |\underline{z}| + 2|\underline{x}(\underline{x} + \underline{z}) + \underline{y}(\underline{y} + \underline{z})| .$$

Furthermore, if $\underline{\ell}_i$ and $\underline{\ell}_2$ denote coset leaders of $\overline{C_3}$ from L and if $f(\underline{\ell}_i)$ and $f(\underline{\ell}_2)$ denote the code words of $\overline{C_3}$ assigned to them in Figure (5.3), then one can easily verify that

$$(5.7)\quad |(\underline{\ell}_1 + \underline{\ell}_2)(\underline{\ell}_1 + \underline{\ell}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))| = 1$$

whenever $|f(\underline{\ell}_1) + f(\underline{\ell}_2)| = 4$.

Now choose any two distinct code words $(\underline{v}_1, \underline{v}_1 + f(\underline{v}_1))$ and $(\underline{v}_2, \underline{v}_2 + f(\underline{v}_2))$ from XNR. The distance between these two words is

$$|(\underline{v}_1 + \underline{v}_2,\ \underline{v}_1 + \underline{v}_2 + f(\underline{v}_1) + f(\underline{v}_2))| .$$

Since Lemma (5.1) implies that $\underline{v}_1 = \underline{\ell}_1 + \underline{m}_1$, $\underline{v}_2 = \underline{\ell}_2 + \underline{m}_2$ for suitable $\underline{\ell}_1$ and $\underline{\ell}_2 \in L$ and $\underline{m}_1$ and $\underline{m}_2 \in \overline{C_3}$, this distance may be written as

$$|(\underline{\ell}_1 + \underline{m}_1 + \underline{\ell}_2 + \underline{m}_2,\ \underline{\ell}_1 + \underline{m}_1 + \underline{\ell}_2 + \underline{m}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))|$$
$$= |f(\underline{\ell}_1) + f(\underline{\ell}_2)| + 2|(\underline{\ell}_1 + \underline{\ell}_2)(\underline{\ell}_1 + \underline{\ell}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))$$
$$+ (\underline{m}_1 + \underline{m}_2)(\underline{m}_1 + \underline{m}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))| \text{ by (5.6).}$$

We examine three cases:

Case 1: $|f(\underline{\ell}_1) + f(\underline{\ell}_2)| = 8$. Clearly, the distance between the two words is greater than or equal to 8 .

Case 2: $|f(\underline{\ell}_1) + f(\underline{\ell}_2)| = 0$. This implies that $\underline{\ell}_1 = \underline{\ell}_2$ and $f(\underline{\ell}_1) = f(\underline{\ell}_2)$. The distance between the two words is

then

$$2|(\underline{m}_1 + \underline{m}_2)(\underline{m}_1 + \underline{m}_2)| = 2|(\underline{m}_1 + \underline{m}_2)| \geq 8$$

because $\underline{m}_1 \neq \underline{m}_2$.

Case 3: $|f(\underline{\ell}_1) + f(\underline{\ell}_2)| = 4$. By (5.7) we now have

$$|(\underline{\ell}_1 + \underline{\ell}_2)(\underline{\ell}_1 + \underline{\ell}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))| = 1 .$$

Since $\underline{m}_1$, $\underline{m}_2$, $f(\underline{\ell}_1)$, and $f(\underline{\ell}_2)$ are in $\overline{C_3}$, $|(\underline{m}_1 + \underline{m}_2)(\underline{m}_1 + \underline{m}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))|$ is an even number. It follows that

$$|(\underline{\ell}_1 + \underline{\ell}_2)(\underline{\ell}_1 + \underline{\ell}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2)) + (\underline{m}_1 + \underline{m}_2)(\underline{m}_1 + \underline{m}_2 + f(\underline{\ell}_1) + f(\underline{\ell}_2))| > 0$$

and the distance is at least 6 .

XNR has $|C| = M = 2^8$ since $\underline{v}$ may be chosen arbitrarily from V(8,2). XNR has distance ≥ 6 since in all three cases above, the distance between any two distinct words of XNR is greater than or equal to 6 . //

(5.8) Any punctured code NR of XNR is called the Nordstrom-Robinson code or NR .

(5.9) Lemma: The NR code is a (15,256,5) code.

Proof: Use (2.5.5), (2.5.8), and Theorem (5.5). //

(5.10) Theorem: The NR code is a nearly perfect (15,256,5) code.

Proof: $2^8 \cdot (1 + \binom{15}{1} + \frac{1}{\lfloor \frac{16}{3} \rfloor} \binom{16}{3}) = 2^{15}$. //

§4.1

A bl

v-se

resp

(1.1

desig

conta

a t-d

and

there

(1.2)

(1.3)

(1.4)

(1.5)

(t - 1)

X {P

CHAPTER 4

t-Design and Generalized Block Intersection Numbers

§4.1 Main Definitions

Let an x-(sub)set denote a (sub)set of cardinality x. A block design is a collection B of k-subsets of a given v-set X. Elements of X and B are points and blocks, respectively.

(1.1) A t-design with parameters λ-(t,k,v) is a block design with the property that each t-subset of X is contained in precisely λ blocks of B. The parameters of a t-design are all non-negative integers so that $0 \leq t \leq k \leq v$ and $\lambda > 0$.

Whenever a t-design with parameters λ-(t,k,v) exists, there exist positive integers b_i, $i = 0,1,\ldots,t$, so that

(1.2) $b_t = \lambda$ and $(v-i)b_{i+1} = (k-i)b_i$ for $0 \leq i < t$.

Some immediate properties of t-designs are:

(1.3) $|B| = b_0 = \lambda \binom{v}{t} / \binom{k}{t}$.

(1.4) A t-design is a (t-1)-design for $t \geq 2$.

(1.5) The blocks of B containing a fixed $P \in X$ form a (t-1)-design with parameters λ-(t-1,k-1,v-1) on the set $X \setminus \{P\}$ as long as $t \geq 2$. This is called the derived

<u>design</u> of the t-design.

Many times one does not know at the outset the value of t for a t-design. Because of this it is useful to define the following for a block design, B, whose point set is X and whose blocks have cardinality k.

(1.6) Define $\hat{b}_i := \underset{\text{over all } i\text{-sets},A}{\text{average}}\{b_A\}$ where b_A is the number of blocks of B containing a given i-set, A.

Then by induction on the cardinality i one can derive formulas analogous to (1.2):

(1.7) $(v-i)\hat{b}_{i+1} = (k-i)\hat{b}_i$ for all $1 \leq i \leq t$.

Since there is only one 0-set, the empty set, $\hat{b}_0 = |B|$ and $= b_0$. From this follows:

(1.8) $\hat{b}_i = |B|\binom{k}{i}/\binom{v}{i}$ for all $0 \leq i \leq k$.

If b_A is constant, independent of which particular t-set, A, is used, $\hat{b}_t = b_A = b_t$ and the block design, B, is by definition a t-design. Example 3 in Section 4.2 shows how (1.8) can be used to obtain the value of t for a t-design.

A t-design with $k = v$ is called <u>trivial</u> and one with $t = k$ is called <u>complete</u>, since in that case B contains all the k-subsets of X, each λ times. Let a <u>complete</u> $\binom{v}{t}$-<u>design</u> denote a $1\text{-}(t,t,v)$ design. If $0 < t < k < v$, the t-design is called <u>incomplete</u>.

(1.9) A Steiner system, denoted by $S(t,k,v)$, is a $1-(t,k,v)$ design which is incomplete. A t-design with $t = 1$ is often called a tactical configuration. A t-design with $t \geq 2$ is balanced. It follows that an incomplete t-design with $t \geq 2$ is a balanced incomplete block design, (BIBD), when considered as a 2-design.

(1.10) An incidence matrix N of a t-design is a $v \times b_0$ matrix of zeros and ones so that the elements of X are indicated by the rows of N, the blocks of B by the columns of N, and so that a point P of X is contained in a particular block iff the corresponding matrix entry is a one. For a BIBD one has the equations:

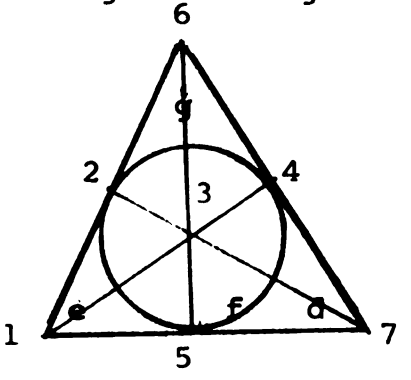
(1.11) $vb_1 = kb_0$ and $(v-1)\lambda = (k-1)b_1$.

If we let J be the matrix of all ones, $\underline{j}$ the column vector of all ones, and I the identity matrix, then equations (1.11) imply

(1.12) $\underline{j}^T N = k\underline{j}^T$, $N\underline{j} = b\underline{j} = b_1\underline{j}$, and $NN^T = (k-\lambda)I + \lambda J$, for any BIBD.

§4.2 Examples

Example 1: As a first example we shall consider the Fano plane, PG(2.2). A drawing of this geometry is given in Figure (2.1):



Let

des

(2.

So

An

Figu

Figu

Exam

the

of

(due

GP(2

this

imme

formu

Letting the points of the geometry be the points of a block design with

(2.2) 1. $v = 7$ points , $b_0 = 7$ blocks (dually:)

2. $k = 3$ points per block , $b_1 = 3$ blocks per point

3. $\lambda = 1$ block determined by two points

So this yields a $1\text{-}(2,3,7)$ design also denoted by $S(2,3,7)$. An incidence matrix for this design corresponding to Figure (2.1) is given in Figure (2.3):

Figure (2.3)

	a	b	c	d	e	f	g
1	0	1	1	0	1	0	0
2	0	0	1	1	0	1	0
3	0	0	0	1	1	0	1
4	1	0	0	0	1	1	0
5	0	1	0	0	0	1	1
6	1	0	1	0	0	0	1
7	1	1	0	1	0	0	0

Q

Example 2: Considering $V(3,2)$ we may choose points to be the 8 vectors of $V(3,2)$. Since the sum of three vectors of $V(3,2)$ is a single and distinct fourth vector of $V(3,2)$ (due to the fact that the sum of two distinct vectors over $GF(2)$ is never null), each triple out of the 8 points of this t-design is contained in a unique block. So we immediately have a $3\text{-}(1,4,8)$ design and can calculate, by formula (1.3)

$$b_0 = 1.\binom{8}{3} / \binom{4}{3} = 14 \text{ dependent 4-sets in } V(3,2).$$

In fact, we have encountered this design earlier in the code $\overline{C_3}$, the extended Hamming code witn parameters $(8,2^4,4)$, (cf. Lemma (2.5.11)). Its incidence matrix was given in Chapter 3 and shall be reproduced in full here, but with the all-one column vector moved to the right end:

Figure (2.4)

P

0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1
0	0	1	1	0	1	0	0	1	0	0	1	0	1	1	1
0	0	0	1	1	0	1	0	1	1	0	0	1	0	1	1
0	0	0	0	1	1	0	1	1	1	1	0	0	1	0	1
0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1
0	0	1	0	0	0	1	1	1	0	1	1	1	0	0	1
0	1	0	1	0	0	0	1	0	1	0	1	1	1	0	1
0	1	1	0	1	0	0	0	0	0	1	0	1	1	1	1

Q R

Notice that P (see Figure (2.4)) is the incidence matrix of all the dependent sets of cardinality 4 and is therefore an incidence matrix for this 1-(3,4,8) or S(3,4,8) design. Furthermore, notice that the incidence matrix Q for the t-design in Example 1 occurs as a sub-matrix. As such, the S(2,3,7) is a derived design from the S(3,4,8) design (cf. (1.5)).

Example 3: Consider once again the Fano plane and this time choose for points and blocks of a new design the points and the sets of 4 points, no three of which are collinear, respectively. Since such sets are co-lines, there are 7

blocks and 7 points in this design. Since co-lines are the complements of lines in PG(2,2) and since two lines meet in at most one point of the geometry, co-lines meet on at most two points. In other words, each triple of points is contained in at most one block (co-line) of the design in question. From (1.8) we have

$$\hat{b}_2 = 7.4.3/7.6 = 2 .$$

Yet, since each triple of points is in at most one block, and since there are only 7 points, each pair of points is contained in at most 2 blocks. Therefore, b_2 is a constant and equals 2 . So this is a 2-(2,4,7) design. An incidence matrix for this design is given by matrix R of Figure (2.4).

§4.3 An Application of t-Designs to Binary Codes

(3.1) Lemma: (Goethals, Snover [17]) Given any nearly perfect e-error correcting code C of length n , with $0 \in C$, the code words of minimum non-zero weight form a $[(n-e)/(e+1)]$ - $(e, 2e+1, n)$ design.

Proof: Let X be the set of coordinate places, and consider the set B of code vectors of weight $d = 2e+1$. Any $x \in B$ determines a d-subset of X , namely the subset of coordinate places where the d ones of $\underline{x}$ are. It follows from Lemma (3.4.13) part (ii) that any e-subset of S is contained in precisely $[(n-e)/(e+1)]$ such d-subsets. //

(3.2) Lemma: (Goethals and Snover [17]) If a punctured code C of code C' of length $n+1$ is a nearly perfect e-error correcting code of length n, and if $\underline{0}' \in \underline{C}'$, then the vectors of weight $d+1 = 2e+2$ in C' determine a $[(n-e)/(e+1)] - (e+1, d+1, n+1)$ design.

Proof: Let X' be the set of $n+1$ coordinate places of the code C' and let P be any fixed place of X'. Let B' be the $(d+1)$-subsets of X determined by the coordinate places in which vectors $\underline{x}' \in C'$ of weight $d+1$ have their $(d+1)$ ones. In order to show that (X', B') is the appropriate $(e+1)$-design, consider the code C of length n obtained from C' by systematically deleting the coordinate associated to P from each of the vectors of C'. Then C is nearly perfect, and according to Lemma (3.1), the vectors at distance d from any vector $\underline{x} \in C$ determine an e-design with parameters $[(n-e)/(e+1)] - (e, d, n)$ on the set $X = X' - \{P\}$. It follows that any $(e+1)$-subset of X containing P is contained in precisely $[(n-e)/(e+1)]$ blocks of (X', B'). Since P may be chosen arbitrarily, the theorem is proved. //

(3.3) Remark: Lemmas (3.1) and (3.2) may be applied to the Golay code and its extension defined in Section 3.3 because of Lemmas (3.3.10) and (3.4.12). Applying them yields 1-(4,7,23) and 1-(5,8,24) designs, i.e. S(4,7,23) and S(5,8,24) Steiner systems.

(3.4) Remark: Likewise, Lemma (3.5.10) implies that Lemmas (3.1) and (3.2) may be applied to the Nordstrom-

Rch

yie

:4.

sev

para

$0 \leq$

of

card

cons

we d

(as

sinc

prec

(blo

a se

thre

ques

of a

the

j-su

inte

Robinson code and its extension (defined in Section (3.5) yielding 4-(2,5,15) and 4-(3,6,16) designs.

§4.4 Block Intersection Numbers $b_{i,j}$

In the first section of this chapter we encountered several constants relating to a t-design. Other than the parameters t,v,k, and b_t were the constants b_i for $0 \leq i \leq t-1$. These are the (integer) counts of the number of blocks of the design passing through any set of cardinality i of points of that design. There are more constants, however, which are worth mentioning.

Let us consider first one example. In Section 4.2 we discussed the 1-(2,3,7) design of points and lines (as blocks) of the Fano plane, PG(2.2). In this geometry, since there are three lines through each point, there are precisely 4 lines missing each point. Of the four lines (blocks) not passing through a given point, two pass through a second given point and two miss the second point. These three counts are constants independent of the points in question.

Let the symbol $b_{i,j}$ be the (integer) number of blocks of a (fixed) t-design passing through a given i-subset of the point set X of the t-design and avoiding a given j-subset of X. These numbers $b_{i,j}$ are called <u>block intersection numbers</u>, according to J. M. Goethals [16].

blo

(4.

$b_{0,}$

Not

pre

blo

The

$0 \leq i$

Lemm

(4.3

(4.4

of t

$0 \leq i$

(4.5

Proo

is ø

proc

and

a co

Assu

Assu

In the example of points and lines of PG(2,2) the block intersection numbers are:

(4.1) $b_{0,0} = 7$

$b_{0,1} = 4$ $\qquad$ $b_{1,0} = 3$

$b_{0,2} = 2$ $\qquad$ $b_{1,1} = 2$ $\qquad$ $b_{2,0} = 1$

Notice that the numbers $b_{i,0}$ are exactly the numbers b_i previously defined since the $b_{i,0}$ means the number of blocks passing through an i-set and avoiding the empty set.

The block intersection numbers are integers by definition. The counts $b_{i,j}$ are well-defined constants as long as $0 \leq i + j \leq t$ and we prove this in the following lemma.

Lemma: The block intersection numbers $b_{i,j}$ satisfy:

(4.3) $b_{i,0} = b_i$ for $0 \leq i \leq t$,

(4.4) $b_{i,j}$ are constants (hence well-defined) independent of the particular i-set and j-set in question as long as $0 \leq i + j \leq t$,

(4.5) (Pascal Property) $b_{i,j} = b_{i+1,j} + b_{i,j+1}$ for $i+j \leq t-1$.

Proof: Property (4.3) is immediate since the only 0-set is $\emptyset$. In order to prove properties (4.4) and (4.5), we proceed by double induction on $s = i + j$ and on $k = j$ and establish both simultaneously. For $s = 0$, $b_{0,0} = b_0 =$ a constant.

Assume for all $i + j \leq s - 1 < t$ that $b_{i,j}$ is constant.

Assume also for all $i + j \leq s - 2 < t$ that

The

Con

For

Ass

the

we

Let

giv

and

$b_{A,}$

But

Pur

by

b_{s-}

and

And

unle

orig

$$b_{i,j} = b_{i+1,j} + b_{i,j+1} \quad .$$

Then consider s so that $s \leq t$.

Considering $b_{s-k,k}$ we further proceed by induction on k .

For $k = 0, b_{s-k,k} = b_{s,0} = b_s$ and is constant.

Assuming for all $k < k_0$ that $b_{s-k,k}$ is constant and

$$b_{s-k-1,k-1} = b_{s-k,k-1} + b_{s-k-1,k} ,$$

then consider b_{s-k_0,k_0-1} . In order to evaluate this, we define the following.

Let $b_{A,B}$ denote the number of blocks passing through a given set A and avoiding a given set B, for $|B| = k_0-1$, and $A \cap B = \emptyset$. By the induction hypotheses we have $b_{A,B} = b_{s-k_0,k_0-1}$.

But for any $P \notin A \cup B$,

$$b_{A,B} = b_{A \cup \{P\},B} + b_{A,B \cup \{P\}} .$$

Furthermore, $b_{A \cup \{P\},B} = b_{s-k_0+1,k_0-1}$ which is a constant by the induction hypothesis. Hence, $b_{s-k_0} = b_{A,B \cup \{P\}} = b_{s-k_0,k_0-1} - b_{s-k_0,k_0-1}$ and is constant. This proves (4.4) and (4.5). //

Properties (4.3), (4.4), and (4.5) require $i + j \leq t$. And the counts $b_{i,j}$ for $i + j > t$ are never constants unless the t-design was actually an $(i + j)$-design originally.

We conclude this section by revisiting the example of

the 14 planar 4-tuples in $V(3,2)$. The counts $b_0 = 14$, $b_1 = 7$, $b_2 = 3$, and $b_3 = 1$ can be found from the three equations of (1.2) and the parameters $1\text{-}(3,4,8)$ of the design. Then noting that $b_{i,0} = b_i$ for $0 \leq i \leq t = 3$, and employing the Pascal property for block intersection numbers we find the $b_{i,j}$ for this design to be:

(4.6)
$$\begin{array}{ccccccc} & & & 14 & & & \\ & & 7 & & 7 & & \\ & 3 & & 4 & & 3 & \\ 1 & & 2 & & 2 & & 1 \end{array} .$$

To help clarify these counts, the number 4 is the count $b_{1,1}$ and represents the number of dependent 4-tuples of $V(3,2)$ containing a given point (vector) $\underline{v_1}$ of $V(3,2)$ and missing another given point $\underline{v_2}$. Choosing any third point of $V(3,2)$, say $\underline{v_3}$, then there are two blocks containing $\underline{v_1}$, missing $\underline{v_2}$ and containing $\underline{v_3}$ and two blocks containing $\underline{v_1}$, missing $\underline{v_2}$ and also missing $\underline{v_3}$. These counts are $b_{2,1} = 2$ and $b_{1,2} = 2$, respectively. Note that the Pascal property $b_{2,1} + b_{1,2} = b_{1,1}$ holds.

§4.5 Motivation for the Generalized Block Intersection Numbers Using the Design of the Thirty 3-Cubes in the 4-Cube

Although in a t-design the counts $b_{i,j}$ are not constant for $i + j > t$ (unless the t-design were originally at least a $(i+j)$-design), these counts may depend only on a certain character of the $(i+j)$-set in question. For example, in $V(3,2)$ the count of the number of dependent 4-sets passing

through a given 4-set is either 1 or 0 depending upon whether that 4-set be a dependent 4-set or an independent one. In the next section we shall define generalized block intersection numbers which are constants, like the block intersection numbers, as long as we specify the particular $(k+j)$-set in question. However, we now preempt that discussion by exploring in depth one important example.

Consider the thirty 3-cubes contained in the 4-cube. That is, consider the thirty copies of $V(3,2)$ contained in $V(4,2)$. That there are thirty is established in the following lemma.

(5.1) Lemma: There are 30 copies of $V(3,2)$ in $V(4,2)$.

Proof: First notice that each $V(3,2)$ contains 14 dependent 4-tuples and hence $\binom{8}{4} - 14 = 56$ independent 4-tuples. Now count the ways to choose an independent 4-tuple from $V(4,2)$. The first three vectors of $V(4,2)$ may be chosen arbitrarily. But then the fourth, in order to form an independent 4-set must not be the unique vector sum of the first three. Since these four vectors from $V(4,2)$ may be chosen in any order, we obtain

$$\frac{16.15.14.12}{4.3.2.1} = 1680 \text{ independent 4-tuples in } V(4,2).$$

Finally, because each $V(3,2)$ contains 56 of these independent 4-tuples, there are in total $1680/56 = 30$ copies of $V(3,2)$ in $V(4,2)$. //

Consider now the t-design whose points are the 16 vectors

of $V(4,2)$ and whose blocks are the 30 copies of $V(3,2)$ in $V(4,2)$.

(5.2) Claim: This design of the thirty 3-cubes in the 4-cube as blocks and the sixteen vectors of the 4-cube as points is a $3-(3,8,16)$ design.

Proof: The key to this proof rests on an inspection of the planar 4-tuples, which are copies of $V(2,2)$. To this end we note the following:

(5.3) Remark: Each pair of $V(3,2)$ can intersect in either a $V(-1,2) = \emptyset$, a $V(0,2)$, a $V(1,2)$, or a $V(2,2)$ and hence the intersection set has cardinality $0,1,2,$ or 4.

Now proceeding with the proof of (5.2) we note that any planar 4-tuple is contained in at most three copies of $V(3,2)$, since the sets of the four points other than the planar 4-tuples from each of the $V(3,2)$ must be disjoint. So each triple is contained in a unique planar 4-tuple.

Next considering formula (1.8) for t-designs we have:

$$\text{average } b_3 = \hat{b}_3 = b_0\binom{k}{3}/\binom{v}{3} = 30.8.7.6/16.15.14 = 3.$$

Finally, since no triple can be contained in more than three blocks, we see that each triple is contained in exactly three blocks, making the design a $3-(3,8,16)$ design.

Now the formulas (1.2) and $v = 16$, $k = 8$, and $b_3 = 3$, imply that $b_0 = 30$, $b_1 = 15$, and $b_2 = 7$. From the Pascal property the block intersection numbers for any $3-(3,8,16)$ design follow:

(5.4)

$$\begin{array}{ccccccc} & & & 30 & & & \\ & & 15 & & 15 & & \\ & 7 & & 8 & & 7 & \\ 3 & & 4 & & 4 & & 3 \end{array}$$

This design of the 30 copies of $V(3,2)$ in $V(4,2)$ is not a 4-design. Indeed, although each planar 4-tuple is contained in three blocks (3-cubes), each non-planar (independent) 4-tuple spans a unique 3-cube. Hence b_4 is non-constant. Note that $\hat{b}_4$ is not even an integer:

$$(5.5) \qquad \hat{b}_4 = \frac{14.3 + 56.1}{70} = \frac{7}{5} ,$$

since each of the 14 planar 4-sets is contained in three blocks and each of the 70-14 = 56 non-planar 4-sets is contained in just one block.

So there are two types of 4-tuples in $V(4,2)$: planar and non-planar 4-tuples. However, the number of blocks through any type of 4-set is a constant. Therefore, it makes sense to define $b_4^P = 3$, and $b_4^N = 1$, for the planar, and non-planar 4-sets respectively. This leads to a generalization of the $b_{i,j}$ w.r.t. the planar set P by defining

$$b_{i,j}^P = b_{i,j} \quad \text{for} \quad i + j \leq 3 ,$$

$$b_{4,0}^P = b_4^P = 3$$

and

$$b_{i,j+1}^P + b_{i+1,j}^P = b_{i,j}^P \quad \text{for} \quad i + j = 3 ; 0 \leq i,j \leq 3 .$$

This last statement defined all $b_{i,j}^P$ for $i + j = 4$ and

for $4 \geq j \geq 1$. These $b^P_{i,j}$ then are:

(5.6)

30

15 15

7 8 7

3 4 4 3

3 0 4 0 3

Similarly we can extend the $b_{i,j}$ to $b^N_{i,j}$:

(5.7)

30

15 15

7 8 7

3 4 4 3

1 2 2 2 1 .

Suppose we try extending the $b_{i,j}$ to other sets L . For example, let L be a dependent 6-tuple in V(4,2) . (In the following chapter we establish the existence of 448 of these.) A dependent 6-tuple has certainly no subset of 4 points which are also dependent (since then the remaining pair of points could not be distinct by (2.2.3) and (2.2.4)). Hence, a dependent 6-tuple contains no planar 4-sets. Then each 4-set contained in the 6-tuple, being an independent set of 4 vectors of V(4,2) , spans a unique V(3,2) . Furthermore, if a 5-set contained in this dependent 6-set were contained in a V(3,2) , the 5-set would then contain a dependent 4-set; so each 5-set contained in the dependent 6-set must span all of V(4,2) .

Actually, we have proved the following lemma which will be useful in Chapter 5:

(5.8) Lemma: Dependent 6-tuples contained in $V(4,2)$ are composed of 6 vectors of $V(4,2)$ no 4 of which are dependent (form a $V(2,2)$) and no 5 of which are contained in a 3-cube (span a $V(3,2)$) .

We may now define $b_4^L = 1$, $b_5^L = 0$, $b_6^L = 0$ (well-defined so long as the set L is a dependent 6-set in $V(4,2)$). Then we may generalize the $b_{i,j}$ to $b_{i,j}^L$ for $0 \leq i+j \leq 6$ by defining

$$b_{i,j}^L = b_{i,j} \qquad \text{for } 0 \leq i+j \leq 3 ,$$

$$b_{i,0}^L = b_i^L \qquad \text{for } 0 \leq i \leq 6 ,$$

and

$$b_{i+1}^L + b_{i,j+1}^L = b_{i,j} \qquad \text{for } 0 \leq i+j \leq 5 .$$

The numbers $b_{i,j}^L$ now count the number of blocks of the 3-(3,8,16) design passing through a given i-set and avoiding j-set where the $(i+j)$-set is a subset of the special set L, namely a dependent 6-tuple from $V(4,2)$. These $b_{i,j}^L$ are:

(5.9)

			30					
		15		15				
	7		8		7			
3		4		4		3		
	1		2		2		1	
0		1		1		1		0
	0		0		1		0	

Our use of these generalized block intersection numbers lies in the interpretation of the bottom line, the $b_{i,j}^L$

for $i+j = 6$:

(5.10) Lemma: A given dependent 6-tuple of $V(4,2)$ meets any copy of $V(3,2)$ in $V(4,2)$ in exactly two or four places.

Proof: Each $b^L_{i,j}$ for $i+j = |L|$ counts the number of blocks of the design in question passing through exactly i (and not the other j) of the points of L. Since in (5.4) only $b^L_{4,2}$ and $b^L_{2,4}$ are non-zero, the lemma follows.//

Finally we shall extend the $b_{i,j}$ to the counts $b^B_{i,j}$ where B is a block of the design.

We already calculated, in (5.5), that each 4-tuple contained in an block of this 3-(3,8,16) design was contained in 7/5 blocks, on the average. Each 5-set, which is contained in a block, a $V(3,2)$, certainly contains an independent 4-set, so this 5-set is contained in only that block, and no other. Therefore, we may set

$$b^B_4 = \hat{b}_4 = 7/5\,, \quad b^B_5 = 1 = b^B_6 = b^B_7 = b^B_8\,.$$

Then again by the definitions:

$$b^B_{i,j} = b_{i,j} \qquad \text{for} \quad 0 \le i+j \le 3$$

$$b^B_{i,0} = b^B_i \qquad \text{for} \quad 0 \le i \le 8$$

$$b^B_{i+1,j} + b^B_{i,j+1} = b_{i,j} \qquad \text{for} \quad 0 \le i+j \le 8\,,$$

we obtain generalized block intersection numbers for this design relative to a block of the design:

(5.11)

30

15 15

7 8 7

3 4 4 3

7/5 8/5 12/5 8/5 7/5

1 2/5 6/5 6/5 2/5 1

1 0 2/5 4/5 2/5 0 1

1 0 0 2/5 2/5 0 0 1

1 0 0 0 2/5 0 0 0 1

Now interpreting these generalized intersection numbers we have:

(5.12) Lemma: Blocks of the 3-(3,8,16) design of the thirty 3-cubes in the 4-cube meet one another in 0 or 4 places.

Proof: Only the $b^B_{i,j} \neq 0$ with $i + j = 8 = |B|$ for $i = 0, 4,$ or 8. That $b^B_{8,0} = 1$ means that the block B of the design meets only itself in all of its 8 places. //

This lemma was not evident a priori. Compare (5.3) to the statement of Lemma (5.12).

(5.13) Note also that we do not wish to consider the generalized numbers $b^B_{i,j}$ to be integers, but rather average over all i-sets of the number of blocks through each i-set contained in the given set B.

§4.6 Generalized Block Intersection Numbers

J. M. Goethals in [16] defined the block intersection numbers $b_{i,j}$ for a t-design and for $0 \leq i + j \leq t$. The generalized block intersection numbers $b^L_{i,j}$ for L being a

block of the design were considered by N. S. Mendelsohn in [25]. These numbers $b^L_{i,j}$, to be formally defined in this section, provide a link between the two concepts as well as a legitimate generalization of both.

Remembering the comment (5.13) at the end of the last section we shall define, relative to a given L set (contained in the point set X of a t-design), $b^L_{i,j}$ as the average over all the possible $(i+j)$-sets contained within L of the number of blocks of the t-design passing through the i-set and avoiding the j-set.

Formally:

(6.1) Let $b^L_{B,A\setminus B}$ denote the integer number of blocks of a given t-design containing all points of A and no points of B, for given sets so that $B \subset A \subset L$.

(6.2) Then

$$b^L_{i,j} := \binom{|L|}{i+j} \sum_{\substack{A\subset L \\ |A|=i+j}} \left(\binom{|A|}{i}^{-1} \sum_{\substack{B\subset A \\ |B|=i}} b^L_{B,A\setminus B} \right) .$$

So the numbers $b^L_{B,A\setminus B}$ are integer counts whereas the $b^L_{i,j}$ are averages over all the possible $b^L_{B,A\setminus B}$ with $B \subseteq A \subseteq L$. (Relative to the very last example in the last section with the set L being a block of the thirty 3-cubes in the 4-cube design, $b^L_{P,P} = 3$, $b^L_{N,N} = 1$, and $b^L_{4,0} = 7/5$ where the sets P and N were the planar and non-planar 4-sets contained in the block L, respectively.)

(6.3) Lemma: The generalized block intersection numbers $b^L_{i,j}$ satisfy:

(6.4) $b^L_{i,j} = b_{i,j}$ for $|L| \leq t$

(6.5) $b^L_{i,j}$ are constants depending only on the particular set L and the cardinalities i and j, and

(6.6) (Pascal Property) $b^L_{i+1,j} + b^L_{i,j+1} = b^L_{i,j}$ for $i + j \leq |L| - 1$.

Proof: Since the $b^L_{B,A\setminus B}$ are constants independent of the set L and the cardinality of B, as long as $|B| \leq t$, property (6.4) is clear. Again, since the $b^L_{i,j}$ are averages over all the possible subdivisions of the given set L, into subsets of cardinality i,j, and $(|L|-i-j)$, these numbers are constants dependent only on the set L and the cardinalities i and j.

Property (6.6) is established directly.

$$b^L_{i,j} = \binom{|L|}{i+j}^{-1} \sum_{\substack{B\subset L \\ |B|=i+j}} \binom{i+j}{i}^{-1} \sum_{\substack{C\subset B \\ |C|=i}} b^L_{C,B\setminus C} \quad \text{by}$$

definition.

Since for each $P \in L\setminus B$ the following holds:

$$b^L_{C,B\setminus C} = b^L_{C\cup P} + b^L_{C,(B\cup P)\setminus C}(B\cup P) \setminus (C\cup P)$$

we can write

$$b^L_{i,j} = \binom{|L|}{i+j}^{-1} \sum_{\substack{B\subset L \\ |B|=i+j}} \binom{i+j}{i} \sum_{\substack{C\subset B \\ |C|=i}} \binom{|L|-(i+j)}{1}^{-1}$$

$$\sum_{P\in L\setminus B} (b^L_{(C\cup P),(B\cup P)\setminus(C\cup P)} + b^L_{C,(B\cup P)\setminus C}),$$

where $C\cup P$ means $C\cup\{P\}$.

Since $\binom{|L|}{i+j+1}\binom{i+j+1}{1} = \binom{|L|}{i+j}\binom{|L|-(i+j)}{1}$

and since

$$\sum_{\substack{B\subset L\\ |B|=i+j}} \sum_{P\in L\setminus B} = \sum_{\substack{A\subset L\\ |A|=i+j+1}} \sum_{P\in A} \quad \text{for} \quad A = B\cup P \ ,$$

$$b^L_{i,j} = \binom{|L|}{i+j+1}^{-1}\binom{i+j+1}{1}^{-1} \sum_{\substack{A\subset L\\ |A|=i+j+1}} \sum_{P\in A} \binom{i+j}{i}^{-1}$$

$$\sum_{\substack{C\subset A\setminus P\\ |C|=i}} \left(b^L_{(C\cup P),A\setminus(C\cup P)} + b^L_{C,A\setminus C}\right) .$$

Then by separation:

$$b^L_{i,j} = \binom{|L|}{i+j+1}^{-1} \sum_{\substack{A\subset L\\ |A|=i+j+1}} \binom{i+j+1}{1}^{-1} \sum_{P\in A} \binom{i+j}{i}^{-1}$$

$$\sum_{\substack{C\subset A\setminus P\\ |C|=i}} b^L_{(C\cup P),A\setminus(C\cup P)} + \binom{|L|}{i+j+1}^{-1} \sum_{\substack{A\subset L\\ |A|=i+j+1}} \binom{i+j+1}{1}^{-1}$$

$$\sum_{P\in A} \binom{i+j}{i}^{-1} \sum_{\substack{C\subset A\\ |C|=i}} \sum_{P} b^L_{C,A\setminus C} .$$

Now, since

$$\binom{i+j+1}{1}\binom{i+j}{i} = \binom{i+j+1}{i+1}\binom{i+1}{1} = \binom{i+j+1}{i}\binom{j}{1}$$

and since

$$\sum_{P\in A}\sum_{\substack{C\subset A\setminus P\\ |C|=i}} = \sum_{\substack{C\subset A\\ |C|=i}}\sum_{P\in A\setminus C} ,$$

$$b^L_{i,j} = \binom{|L|}{i+j+1}^{-1} \sum_{\substack{A\subset L\\ |A|=i+j+1}} \binom{i+j+1}{i+1}^{-1}\binom{i+1}{1}^{-1}$$

$$\sum_{\substack{C\subseteq A\\ |C|=i}} \sum_{P\in A\setminus C} b^L_{(C\cup P),A\setminus(C\cup P)} + \binom{|L|}{i+j+1}^{-1}$$

$$\sum_{\substack{A\subseteq L\\ |A|=i+j+1}} \binom{i+j+1}{1}^{-1} \binom{j}{1}^{-1} \sum_{\substack{C\subseteq A\\ |C|=i}} \sum_{P\in A\setminus C} b^L_{C,A\setminus C} \cdot$$

Furthermore, $\sum_{\substack{C\subseteq A\\ |C|=i}} \sum_{P\in A\setminus C} \sum_{\substack{D\subseteq A\\ |D|=i+1}} \sum_{P\in D}$ for $D = C\cup P$ yield

$$b^L_{i,j} = \binom{|L|}{i+j+1}^{-1} \sum_{\substack{A\subseteq L\\ |A|=i+j+1}} \binom{i+j+1}{i+1}^{-1} \sum_{\substack{D\subseteq A\\ |D|=i+1}} \binom{i+1}{1}^{-1}$$

$$\sum_{P\in D} b^L_{D,A\setminus D} + \binom{|L|}{i+j+1}^{-1} \sum_{\substack{A\subseteq L\\ |A|=i+j+1}} \binom{i+j+1}{i}^{-1}$$

$$\sum_{\substack{C\subseteq A\\ |C|=i}} \binom{j}{1}^{-1} \sum_{P\in A\setminus C} b^L_{C,A\setminus C} \cdot$$

Then since $b^L_{D,A\setminus D}$ is constant for each $P\in D$ and since $b^L_{C,A\setminus C}$ is constant for each $P\in A$ c, $b^L_{i,j} = b^L_{i+1,j} + b_{i,j+1}$. //

Note: If all the $b^L_{i,0}$ can be calculated for a given set L relative to a given t-design, then by the Pascal property (6.6) all $b^L_{i,j}$ can be calculated. Then one may conclude facts from the other $b^L_{i,j}$ for $j \neq 0$, especially those for $i+j = |L|$. This process can work in other ways as well, e.g. if the $b^L_{i,j}$ can be found for $i+j = |L|$ then the $b^L_{i,0}$ may be calculated.

§4.7 t-Designs with $d \geq d_0$

Throughout this thesis we shall deal with various t-designs having the property that $b^L_{t+1,0} = 1$ for every

block L of a design. This property means that each $(t+1)$-set is contained in at most one block, or equivalently that columns of the incidence matrix for the t-design are a distance at least $2(k-t)$ apart when considered as vectors. Hence we have now proved:

(7.1) Lemma: Vector columns of the 0,1 incidence matrix for a t-design have distance $\geq 2(k-t)$ from one another iff $b^L_{t+1,0} = 1$ for the generalized block intersection numbers of the t-design relative to a given block L of the design.

Remarks: If $b^L_{t,0} = 1$ for a given t-design and block L, the design is a Steiner System. A t-design with $b^L_{t+1,0} = 1$ for blocks L is a generalized Steiner system that by Lemma (7.1) has use in coding theory.

Lemma (7.1) now serves as a motivation for the following definition.

(7.2) Define a t-design with $d \geq d_0$ to be a t-design so that the column vectors of the incidence matrix for the design have mutual distance at least d_0.

(7.4) Lemma: The 3-(3,8,16) design of the thirty 3-cubes in the 4-cube is a 3-(3,8,16) design with $d \geq 8$.

Proof: By the $b^L_{i,j}$ in (5.11) we see that $b^L_{5,0} = 1$ so that $d \geq 2(8-4) = 8$. //

As applications and examples of the concept of a t-design with $d \geq d_0$ we establish the following lemmas.

(7.5) Lemma: A vector set of vectors of length v and

all of weight k and of mutual distance $d \geq d_0$ has b_0 vectors with

(7.6) $\quad b_0 \leq [\ \frac{v-t}{k-t}\ ]\binom{v}{t}/\binom{k}{t}$

for $t = (k - \frac{d_0'}{2})$ and $d_0' = 2[\ \frac{d_0+1}{2}\ ]$. (d_0' = smallest even integer greater than or equal to d_0) .

Proof: For t and d_0' defined above (d_0' is the even integer $\geq d_0$), through each t-set can pass at most $[\frac{v-t}{k-t}]$ vectors. Given b_0 vectors, then the average b_t for this system of b_0 vectors is

$$\frac{b_0\binom{k}{t}}{\binom{v}{t}} = \hat{b}_t \leq [\frac{v-t}{k-t}] \quad \text{from (1.8)}$$

since for each particular t-set $b_t \leq [\frac{v-t}{k-t}]$. Solving for b_0 proves the lemma. //

(7.7) Lemma: A vector set of vectors of length v, weight k and mutual distance $d \geq d_0$ and the maximum possible $b_0 = [\frac{v-t}{k-t}]\binom{v}{t}/\binom{k}{t}$ (according to (7.6) is a t-design. If also $[\frac{v-t}{k-t}] = \frac{v-t}{k-t}$, then the t-design is a (t+1)-Steiner system.

Proof: The first part arises from the fact that $b_t \leq [\frac{v-t}{k-t}]$ for any given t-set $\hat{b}_t = [\frac{v-t}{k-t}]$ from the fact that b_0 is maximal. Hence $b_t = [\frac{v-t}{k-t}]$. $d \geq d_0$ ensures that each (t+1)-set is contained in a unique block. If also $[\frac{v-t}{k-t}] = \frac{v-t}{k-t}$, then each (t+1)-set is contained in at least one block. //

One could at this point apply Lemma (7.7) to the GOLAY and NR codes and obtain the same result as stated in (3.3) and (3.4). However, the proof given in Section 4.3 is more

efficient as well as sufficient for our purpose. We shall instead give an example of (7.7) that shall be used later in Chapter 8 .

(7.8) Lemma: If T is maximal set of vectors of V(8,2) of weight 4 and having mutual Hamming distance ≥ 4, then T is a S(3,4,8) design.

Proof: From (7.6), $t = 4 - 4/2 = 2$. Then $b_0 = [\frac{8-2}{4-2}]$. $\frac{8.7}{4.3} = 14$. Equality holds in the inequality (7.6) so by (7.7), the design is a S(3,4,8) . //

Furthermore, one obtains from the generalized block intersection numbers for this S(3,4,8) design T relative to a block of the design:

(7.9) Lemma: T as given in Lemma (7.8) is composed of 7 complementary pairs of vectors, with representatives from distinct complementary pairs having Hamming distance exactly equal to 4 .

Proof: Let L be any block of T , then the generalized block intersection numbers for T relative to L are necessarily:

(7.10)

				14				
			7		7			
		3		4		3		
	1		2		2		1	
1		0		2		0		1

where $b^L_{3,0} = 1 = b^L_{4,0}$ since $d \geq 4$ in this design. In (7.10), $b^L_{0,4} = 1$, so the complement of each block is necessarily a block, all other blocks meet L then at distance exactly equal to 4 . //

It is important to note that this added condition, with $d \geq d_0$, is not necessarily satisfied by a general t-design. Consider for the moment the 4-(3,6,16) design of minimum non-zero weight vectors in an XNR code containing $\underline{0}$ (see Remark (3.4)). Since this design has an incidence matrix whose columns are code words in XNR, and since XNR has minimum distance 6 between code words, the design has the "with $d \geq 6$" property. We have constructed numerous non-isomorphic 4-(3,6,16) designs, but we show (after Chapter 9) that there is only one 4-(3,6,16) design with $\underline{d \geq 6}$; that is, there is only one such design which can be embedded in a code.

(7.3) So that it will be easier to state later theorems we shall call any 4-(3,6,16) design with $d \geq 6$ an <u>XNR-design</u>. One such exists by Theorem (3.9), is explicitly constructed in Chapter 5 and is shown to be unique up to isomorphism in Chapter 9.

CHAPTER 5

Automorphism Groups and an Explicit Construction of the XNR-Design

§5.1 Permutation Groups

Given a finite set X whose elements are called points, a permutation on X is a bijection $x : X \to X$. Under the operation of composition, the set of all permutations on X, S_X, is the symmetric group on X. If X is fixed in a particular discussion and $|X| = n$, we sometimes write S_n for S_X. A transposition is a permutation which fixes all but two of the points of X and exchanges those two points. A permutation can be written as a product of transpositions in numerous ways, but the number modulo 2 of transpositions used is always a constant; hence, a permutation is considered odd or even as the number of transpositions needed is odd or even, respectively. The group of all even permutations of S_X is a normal subgroup of index 2 denoted by A_X or A_n.

A permutation group is a triple (X,G,i), where X is a finite set, G is an abstract finite group, and i is a homomorphic injection $i : G \to S_X$. We say that G acts on X or G has a (permutation) representation on X. If the kernel of the injection is trivial, the representation of G

is faithful and $|X|$ is the degree of the representation. In practice, for faithful representations, we shall identify G with its image in S_X .

An orbit of a point $P \in X$ under the action of G on X is the set

$$xG := \{xg \mid g \in G\} .$$

G is transitive on X if all points of X are in one orbit of the action of G on X . Clearly, G is transitive on any given orbit; and a representative of an orbit is simply any member of the orbit. G is k-transitive on X if for each pair of k-subsets of X , $\{x_1,x_2,\ldots,x_k\}$ and $\{y_1,y_2,\ldots,y_k\} \subset 2^X$, there exists an element $g \in G$ so that

$$x_i g = y_i \quad \text{for} \quad i = 1,2,\ldots,k .$$

Then by definition it is clear that the concepts of "1-transitive" and "transitive" are identical. A group G is half-transitive on X if there are t orbits for $1 < t < |X|$ and each of the orbits has the same cardinality. A regular group G is a group G transitive on X and so that $|G| = |X|$.

§5.2 Automorphism Groups

An $n \times n$ permutation matrix P_n is a matrix obtained from the $n \times n$ identity matrix, I_n , by permuting its columns. Clearly, the set of all permutation matrices is S_n.

(2.1) The group of automorphisms, the automorphism group, $Aut(N)$, of a $v \times b$ incidence matrix N is the set of all permutation matrices P_v for which there exists a corresponding permutation matrix Q_b so that

$$P_v N Q_b = N .$$

The set $\{P_v\}$ is a group under matrix multiplication since for given P_v^i, $i = 1,2$, there exist Q_b^i, $i = 1,2$, so that

$$(P_v^1 P_v^2) N (Q_b^2 Q_b^1) = P_v^1 N Q_b^1 = N .$$

Let $D = (X, B)$ be a t-design.

(2.2) An automorphism group of a t-design D is the group of permutations π of the point set X so that for each $b \in B$, $b\pi \in B$. As a special case of this definition, we state in particular that the automorphism group of a graph is the group of permutations π of the points (vertices) of the graph so that for each edge $\{v_1, v_2\}$, $\{v_1\pi, v_2\pi\}$ is also an edge. One can easily establish the following properties:

(2.3) The automorphism group $Aut(N)$ of an incidence matrix N for a t-design is isomorphic to the automorphism group of the t-design.

(2.4) If N_1 and N_2 are two incidence matrices for a t-design, then $Aut(N_1) \simeq Aut(N_2)$.

(2.5) The automorphism group of a code C is the group of permutations π of the standard basis elements, i.e. the coordinate positions, so that for each $\underline{v} \in C$, $\underline{v}\pi \in C$. Since the incidence matrix of vectors of C can be arranged as a

disjoint union of incidence matrices of vectors of C of each distinct weight class, which matrices are 0-designs, we have

(2.6) Lemma: The automorphism group of a binary code C is the intersection of the groups $\mathrm{Aut}(C_k)$, $\forall_k$.

Proof: Each class C_k of all of the vectors of weight k in C has, as a 0-design a group $\mathrm{Aut}(C_k)$ of automorphisms. Each of these groups acts on X , the set of n coordinate positions. For each π in the automorphism group of C , $\mathrm{Aut}(C)$ holds necessarily $\underline{v}_k \pi = \underline{w}_k \in C$, so $\pi \in C \bigcap_{k=0}^{n} \mathrm{Aut}(C_k)$. Clearly for each $\pi \in \bigcap_{k=0}^{n} \mathrm{Aut}(C_k)$, $\underline{v}\pi \in C$ for each $\underline{v} \in C$, so

$$\mathrm{Aut}(C) = \bigcap_{k=0}^{n} \mathrm{Aut}(C_k) \ . \ //$$

§5.3 Applications and Examples

In this section we shall apply some of the definitions given in Section 5.2 to specific examples. Our goal is to construct from the action of the group of translations of $V(4,2)$ acting on the set of 448 dependent 6-tuples of $V(4,2)$ an XNR-design, [Theorem (3.10)], thus establishing the fact that the group of translations of $V(4,2)$ acts on this design. The XNR-design is a $4\text{-}(3,6,16)$ design with $d \geq 6$ according to Definition (4.7.3).

The points of $V(n,2)$ form an additive abelian group under vector addition.

(3.1) Definition: $T(n)$ is the group of translations on $V(n,2)$, i.e. $T\underline{x} \in T(n)$ is a translation given by

$(\underline{y})T\underline{x} = \underline{y} + \underline{x}$ for each $\underline{y} \in V(n,2)$.

(3.2) Lemma: $T(n)$ acts as a regular group on the points of $V(n,2)$.

Proof: For two points $\underline{y},\underline{x} \in V(n,2)$ then $\underline{z}T\underline{y} = \underline{z}T\underline{x}$ for all $\underline{z} \in V(n,2)$ is equivalent to $\underline{x} = \underline{y}$. Hence, there are exactly $|V(n,2)|$ elements in $T(n)$. But also, for each pair $\underline{y},\underline{x} \in V(n,2)$ there is a vector $(\underline{x}+\underline{y})$, and hence a translation $T(\underline{x}+\underline{y})$, so that $\underline{y}T(\underline{x}+\underline{y}) = \underline{y}+\underline{x}+\underline{y} = \underline{x}$. Hence, $T(n)$ is transitive on the points of $V(n,2)$. //

(3.3) Lemma: In $V(4,2)$ there exist 448 dependent 6-tuples. These as blocks and the 16 vectors of $V(4,2)$ as points form a 6-(3,6,16) design with $d \geq 4$.

Proof: By the Lemma (4.5.8) we can see that in choosing 6 vectors to form a dependent set from $V(4,2)$ the first three may be chosen arbitrarily, so there are 16, 15, and 14 choices for each of these. The fourth must not be the sum of the first three, so this may be chosen in 12 ways. The fifth cannot be in the $V(3,2)$ spanned by the first four, so this may be chosen in 8 ways. The final vector is then the (unique) sum of the first five. So in total there are

$$16.15.14.12.8.1/6! = 448$$

such sets.

Next we notice that an arbitrary triple of vectors from $V(4,2)$ may be completed to a dependent 6-set in

$$12.8.1/3! \text{ ways, i.e. } b_3 = 16 ,$$

since the first three of a dependent 6-set may be completely arbitrarily chosen. So the design is a 16-(3,6,16) design.

Let B_1 and B_2 be any two distinct dependent 6-sets from $V(4,2)$. Their symmetric difference:

(3.4) $B_1 \Delta B_2 := (B_1 \setminus B_2) \cup (B_2 \setminus B_1)$

is also dependent and has even cardinality > 0. Since no pair of distinct vectors over GF(2) are dependent, $|B_1 \Delta B_2| \geq 4$. Hence, the design has $d \geq 4$. //

(3.5) Theorem: T(4) acts on the 448 dependent 6-tuples of points of V(4,2) yielding 28 orbits of 16 dependent 6-tuples per orbit. Each orbit is a 2-(2,6,16) design with $d \geq 8$. Furthermore, T(4) acts half-transitively on these 448 dependent 6-tuples.

Proof: Let

(3.6) $Q := \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4, \underline{x}_5, \underline{x}_6 \mid \sum_{i=6} \underline{x}_i = \underline{0}\}$

be any one of the dependent 6-tuples. Let also

$$A := \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_6, \underline{x}_1 + \underline{x}_2 + \underline{x}_3, \underline{x}_1 + \underline{x}_2 + \underline{x}_4, \ldots, \underline{x}_1 + \underline{x}_5 + \underline{x}_6\}$$

$$B := \{\underline{x}_1 + \underline{x}_2, \underline{x}_1 + \underline{x}_3, \ldots, \underline{x}_5 + \underline{x}_6, \underline{0}\}$$

$$X := \{\underline{x}_1, \underline{x}_2, \ldots, \underline{x}_6, \underline{x}_7, \underline{x}_8, \ldots, \underline{x}_{15}, \underline{0}\} .$$

By simply checking, one sees that $|B| = 16 = |A| = |X|$, whence, $X = A = B$.

(3.7) Let $\underline{y} \in X$, $\underline{y} \neq 0$. Then we claim that

$$|(Q + \underline{y}) \cap Q| = 2 .$$

For $\underline{y} \neq \underline{0}$, there exists a unique non-zero element of B(=X)

so that $\underline{y} = \underline{x}_1 + \underline{x}_2$, say.

Then

$$(Q + \underline{y}) = \{x_2, x_1, x_1 + x_2 + x_3, x_1 + x_2 + x_4, x_1 + x_2 + x_5, x_1 + x_2 + x_6\}$$

and $(Q + \underline{y}) \cap Q = \{x_1, x_2\}$ since $Q + \underline{y} \subset A$.

Hence (3.7) holds. But each non-zero element $\underline{y}$ of X yields (by considering B) a distinct dependent 6-tuple $(Q + \underline{y})$, so orbits under the action of T(4) on the 448 dependent 6-tuples have cardinality $1 + 15 = 16$.

Each pair of points from Q is contained in Q and precisely one other dependent 6-tuple in the orbit of Q under T(4). Since this property holds for each member of the orbit, each pair of points of V(4,2) is contained in precisely two members of the orbit. Hence the 16 dependent 6-tuples in any orbit form a 2-(2,6,16) design. Finally $d \geq 8$ since, in a given orbit, any pair of dependent 6-tuples share precisely two points of V(4,2). //

(3.8) Lemma: For Q being one of the dependent 6-tuples of points of V(4,2) as defined in (3.6) and for any non-zero point $\underline{z} \in V(4,2)$ then

$(Q + \underline{z}) \Delta Q$ in a 3-cube.

Proof: Let $Q := \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4, \underline{x}_5, \underline{x}_6 \mid \sum_{i=1}^{6} \underline{x}_i = \underline{0}\}$

Then by Theorem (3.5), $\underline{z} = \underline{x}_1 + \underline{x}_2$ say and $(Q + \underline{z}) \Delta Q =$

$$= \{\underline{x}_3, \underline{x}_4, \underline{x}_5, \underline{x}_6, \underline{x}_1 + \underline{x}_2 + \underline{x}_3, \underline{x}_1 + \underline{x}_2 + \underline{x}_4, \underline{x}_1 + \underline{x}_2 + \underline{x}_5, \underline{x}_1 + \underline{x}_2 + \underline{x}_6\}.$$

One can easily see that $\underline{x}_3, \underline{x}_4, \underline{x}_5$, and $\underline{x}_6$ are a basis of $(Q + \underline{z}) \Delta Q$ (using $\sum_{i=1}^{6} \underline{x}_i = \underline{0}$).

As such, $(Q + \underline{z}) \Delta Q$ is a copy of $V(3,2)$ within $V(4,2)$ and is therefore by definition a 3-cube. //

(3.9) Theorem: An XNR-design exists with $T(4)$ acting transitively on the 16 points of the design.

Proof: It suffices to construct the 4-(3,6,16) design as a set of 7 disjoint orbits. Consider the following 7 dependent 6-tuples:

$$Q_1 := \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4, \underline{x}_5, \underline{x}_6 \mid \sum_{i=1}^{6} \underline{x}_i = \underline{0}\}$$

$$Q_2 := \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_1 + \underline{x}_2 + \underline{x}_4, \underline{x}_1 + \underline{x}_3 + \underline{x}_5, \underline{x}_1 + \underline{x}_4 + \underline{x}_5\}$$

$$Q_3 := \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_1 + \underline{x}_3 + \underline{x}_6, \underline{x}_1 + \underline{x}_5 + \underline{x}_6, \underline{x}_1 + \underline{x}_2 + \underline{x}_5\}$$

$$Q_4 := \{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_1 + \underline{x}_4 + \underline{x}_6, \underline{x}_1 + \underline{x}_2 + \underline{x}_6, \underline{x}_1 + \underline{x}_3 + \underline{x}_4\}$$

$$Q_5 := \{\underline{x}_4, \underline{x}_5, \underline{x}_6, \underline{x}_1 + \underline{x}_2 + \underline{x}_4, \underline{x}_1 + \underline{x}_3 + \underline{x}_6, \underline{x}_1 + \underline{x}_4 + \underline{x}_6\}$$

$$Q_6 := \{\underline{x}_4, \underline{x}_5, \underline{x}_6, \underline{x}_1 + \underline{x}_3 + \underline{x}_5, \underline{x}_1 + \underline{x}_5 + \underline{x}_6, \underline{x}_1 + \underline{x}_2 + \underline{x}_6\}$$

$$Q_7 := \{\underline{x}_4, \underline{x}_5, \underline{x}_6, \underline{x}_1 + \underline{x}_4 + \underline{x}_5, \underline{x}_1 + \underline{x}_2 + \underline{x}_5, \underline{x}_1 + \underline{x}_3 + \underline{x}_4\} .$$

(3.11) It is straightforward to check that each of these Q_i is a dependent 6-set and that any pair of distinct Q_i meet one another in either 1 or 3 places.

Define D to be the $7.16 = 112$ dependent 6-sets, called blocks of D, obtained from the 7 orbits (of dependent 6-tuples under the action of $T(4)$) whose representatives are Q_i, $i = 1,2,\ldots,7$. Since no 2 of the Q_i meet on exactly 2 places, no 2 of the orbits coincide.

Let, for the moment, Q and R be any 2 distinct dependent 6-tuples from among the 448 in $V(4,2)$. Let $\underline{z}$

be any non-zero point of $V(4,2)$, then Lemmas (3.8) and (4.5.9) imply

$$|Q \cap ((R + \underline{z}) \Delta R)| = 2 \text{ or } 4 .$$

Therefore

$$|Q \cap ((R + \underline{z}) \Delta R)| = 0 \bmod 2 .$$

But $$|Q \cap ((R + \underline{z}) \Delta R)| = |(Q \cap (R + \underline{z})) \Delta (Q \cap R)|$$

$$= |Q \cap (R + \underline{z})| + |Q \cap (R + \underline{z}) \cap R| ,$$

so that

(3.12) $|Q \cap R| = |Q \cap (R + \underline{z})|$ modulo 2 .

Now letting Q and R be blocks of D, (3.11) and (3.12) imply that by considering the representatives for Q and R among $\{Q_i\}$, $i = 1,2,\ldots,7$,

(3.13) $|Q \cap R| \equiv 1$ modulo 2

iff Q and R are in distinct orbits.

If Q and R are in the same orbit then, by Theorem (3.5), $|Q \Delta R| = 8$. If Q and R are in different orbits then, by (3.4) and (3.13), $|Q \Delta R| = 10$ or 6. Therefore

(3.14) $d \geq 6$ in this design.

Finally (3.14) together with Lemma (4.7.7) imply that D is a $4\text{-}(3,6,16)$ design with $d \geq 6$, i.e. by Definition (4.7.3), D is an XNR-design. Now Theorem (3.9) is proved. //

PART C: THE NORDSTROM-ROBINSON CODE

CHAPTER 6

Equivalence of the Uniqueness of the XNR Code and the Uniqueness of the XNR-Design

§6.1 Introduction

The method of constructing the extended Nordstrom-Robinson cede, XNR, given in Theorem (3.5.4) is not the only one. J. M. Goethals demonstrated [15] that such a code could be derived from the XGOLAY code. From his work with these codes, Goethals suggested in a private communication that the Nordstrom-Robinson code might be unique. Thanks to his suggestion, we now show that this conjecture is true.

Our long proof of the uniqueness of XNR (and NR) is subdivided for convenience into chapters. In this chapter we reduce the question of uniqueness of these codes to that of the uniqueness of the XNR-design, which was defined in (4.7.3). It is then shown that every XNR-design can be described in terms of the geometry of $V(4,2)$. In Chapters 8 and 9 we show that within $V(4,2)$ the XNR-design is unique up to an automorphism of $Aut(V(4,2))$. Finally Chapter 10 is a summary of the various parts of the uniqueness proof.

§6.2 Organization of Chapter 6

This chapter is organized as follows. In Section 6.3 it is shown [Theorem (3.1)] that the set of minimum non-zero weight vectors in any (16,256,6) code, C, with $\underline{0} \in C$ form an XNR-design. Section 6.4 establishes the necessary weight distribution of any (16,256,6) code, C, with $\underline{0} \in C$, and shows that the vectors of weights 10 and 16 in C are the complementary vectors to those of weights 6 and 0. In Section 6.5 it is shown that the vectors of weight 8 in C must necessarily be obtained from the XNR-design in a special way. The equivalence of the questions of uniqueness of the (16,256,6) code and the XNR-design is then stated in Section 6.6.

§6.3 The Fundamental XNR-Design of Weight 6 Code Words in any (16,256,6) Code C, with $\underline{0} \in C$.

Note that there is no loss of generality in assuming that any (16,256,6) code contains $\underline{0}$, since if C* is a (16,256,6) code with $\underline{x}^* \in C^*$, then $C := C^* + \underline{x}^*$ is an equivalent code with $\underline{0} = \underline{x}^* + \underline{x}^* \in C$.

(3.1) Theorem: In any (16,256,6) code C, with $\underline{0} \in C$, the set of 112 weight 6 code words forms an XNR-design.

Proof: Since $256 \cdot \left(1 + \binom{16-1}{1} + \frac{1}{\left[\frac{16}{3}\right]} \binom{16}{3} \right) = 2^{(16-1)}$, any punctured code of C is nearly perfect, by (3.4.11). Then by Lemma (4.3.2), the set of weight 6 code words form a 4-(3,6,16) design with $d \geq 6$, which is, by

Definition (4.7.3) an XNR-design. Finally this design has $b_0 = 4\binom{16}{3}/\binom{6}{3} = 112$ blocks by (4.1.3). //

§6.4 The Weight Distribution of any (16,256,6) code, C, with $\underline{0} \in C$

(4.1) Theorem: Any (16,256,6) code, C, with $\underline{0} \in C$ has 112 code words of weights 6 and 10, 30 words of weight 8, and one code word of weight 16. Such a code has the additional property that the complementary vector to any code word is also a code word.

Proof: Let C be any (16,256,6) code with $\underline{0} \in C$. Since vector addition is done modulo 2, $\underline{0} \in C + \underline{z}$ for any coset code $C + \underline{z}$. For this reason, for each $\underline{z} \in C$, $C + \underline{z}$ is a (16,256,6) code with $\underline{0} \in C + \underline{z}$. Theorem (3.1) then applies also to $C + \underline{z}$ showing (4.2) lemma. The 112 weight 6 code words in any $C + \underline{z}$, for $\underline{z} \in C$, are the elements of an XNR-design. This is the key point in the proof of Theorem (4.1). Indeed, many of the proofs of the following lemmas, which eventually prove Theorem (4.1), consider the generalized block intersection numbers for the XNR-design indicated by the weight 6 code words of a $C + \underline{z}$ coset code for a particular $\underline{z} \in C$.

Useful in establishing the various generalized block intersection numbers needed are the block intersection numbers for any 4-(3,6,16) design:

(4.3)

$$\begin{array}{ccccccc} & & & 112 & & & \\ & & 70 & & 42 & & \\ & 42 & & 28 & & 14 & \\ 24 & & 18 & & 10 & & 4 \end{array} .$$

We shall now proceed with the series of lemmas which culminate in Theorem (4.16), a restatement of Theorem (4.1). The following two lemmas will be proved simultaneously.

(4.4) Lemma: Any (16,256,6) code, C , with $\underline{0} \in C$ contains 15 weight 8 code words, no two of which are complementary.

(4.5) Lemma: Any (16,256,6) code, C , with $\underline{0} \in C$ contains at least 36 weight 10 code words.

Proofs of Lemmas (4.4) and (4.5): Let $\underline{z} \in C$ be a code word of weight 6 . By Theorem (3.1), the 112 weight 6 code words in $C + \underline{z}$ indicate an XNR-design. Also in the coset code $C + \underline{z}$ is the code word $\underline{z}$. Let L be the 6-tuple indicated by the vector $\underline{z}$. Consider now the generalized block intersection numbers for the XNR-design relative to L . Since the design has $d \geq 6$, (cf. Definition (4.7.3)), $b^{L}_{4,0} = 1$ for each block L . Therefore these numbers, $b_{i,j}$, are the same relative to any block of any XNR-design, and are:

(4.6)

$$\begin{array}{ccccccc} & & & 112 & & & \\ & & 70 & & 42 & & \\ & 42 & & 28 & & 14 & \\ 24 & & 18 & & 10 & & 4 \\ & 13 & & 11 & & 7 & & 3 & & 1 \\ & & 6 & & 7 & & 4 & & 3 & & 0 & & 1 \\ & & & 0 & & 6 & & 1 & & 3 & & 0 & & 0 & & 1 \end{array}$$

From these numbers, the $b^{L}_{i,j}$ with $i+j=6$ imply that $6 \times \binom{6}{1} = 36$ blocks of the design meet L in one place, $1 \times \binom{6}{2} = 15$ blocks meet L in two places, and $3 \times \binom{6}{3} = 60$ blocks meet L in three places. Therefore, of the 112 weight 6 code words in $C+\underline{z}$, one is $\underline{z}$ and the 36,15, and 60 others are at distances 10, 8, and 6 from $\underline{z}$, respectively.

Adding the vector $\underline{z}$ to each of these 112 weight 6 code words of $C+\underline{z}$, we obtain code words in $C = C+\underline{z}+\underline{z}$. Therefore C contains $\underline{0}$, at least 36 code words of weight 10, and at least 15 code words of weight 8. The 15 weight 8 code words could not have any pair being complemented, for then the corresponding pair upon addition of $\underline{z}$, would be a pair of weight 6 vectors in $C+\underline{z}$ at a distance 16 from each other. This is a contradiction, since the distance between two weight 6 vectors is at most 12. Lemmas (4.4) and (4.5) are thus proved.

(4.7) Lemma: C contains no code word of weight 12.

Proof: Consider the XNR-design relative to the 112 weight 6 code words in C. Let $\underline{w}$ be any weight 12 vector. Then $\underline{j}+\underline{w}$ is a vector of weight 4, for $\underline{j}$ the all one vector of length 16. Now $\underline{j}+\underline{w}$ indicates the 4-tuple, M, which gives these generalized block intersection numbers, $b_{i,j}$, for this design:

(4.8)

			112		
		70		42	
	42		28		14
24		18		10		4
12+x	12+x		6+x		4-x	x

where $b^M_{4,0} = x = 0$ or 1. This means that any such 4-tuple, M, is disjoint from at least 12 blocks of the design. Hence, $\underline{w}$ contains at least 12 weight 6 code words of C.

Let $\underline{z}$ be one of these 12 weight code words of C. Then in $C + \underline{z}$, $\underline{w} + \underline{z}$, and $\underline{z}$ are code words located at distance 12, contradicting $b^L_{0,6} = 0$ in (4.6). From this contradiction follows the fact that $\underline{w}$ cannot be a code word of C. Since $\underline{w}$ is an arbitrary weight 12 vector, Lemma (4.7) is proved.

(4.9) Lemma: Any weight 10 code word in any (16,256,6) code, C, with $\underline{0} \in C$, is the complement of a weight 6 code word in C.

Proof: Consider any weight 10 vector $\underline{v}$. Viewing the complementary weight 6 vector, $\underline{j} + \underline{v}$, as a 6-tuple, N, in the XNR-design of the 112 weight 6 code words of C, we obtain these $b^N_{i,j}$:

(4.10)

$$
\begin{array}{ccccccc}
 & & & & & & 112 \\
 & & & & & 70 & 42 \\
 & & & & 42 & 28 & 14 \\
 & & & 24 & 18 & 10 & 4 \\
 & & 12+x & 12-x & 6+x & 4-x & x \\
 & 2+5x-y & 10-4x+y & 2+3x-y & 4-2x+y & x-y & y \\
-10+15x-6y+z & 12-10x+5y-z & -2+6x-4y+z & 4-3x+3y-z & x-2y+z & y-z & z \, .
\end{array}
$$

Now, a weight 10 code vector $\underline{v}$ cannot meet any weight 6 code word at distance 12, since then $C + \underline{v}$ would be a (16,256,6) code with $\underline{0} \in C$ and containing a code word of

weight 12, contradicting Lemma (4.7) . Hence,

(4.11) $0 = b^N_{0,6} \; -10 + 15x - 6y + z$ and

(4.12) $0 = b^N_{4,2} \; x-2y+z$.

Notice that z is an integer, because $b^N_{6,0}$ is simply the number of blocks meeting the set N in all of its points. Moreover, $z = 1$ or 0 , because the 6-set N is either a block or not. These equations (4.11) and (4.12) together with $z = 1$ or 0 yield the following two possible sets of solutions:

Case 1: $x = y = z = 1$. Hence, the 6-tuple N represents a block, i.e. the vector $\underline{v}$ is the complement of a weight 6 code vector.

Case 2: $z = 0$, $y = 5/12$, $x = 5/6$. This implies that the 6-tuple meets:

$$(y-z).\binom{6}{5} = (5/12).6 = 5/2$$

blocks of the design in five places. But since $5/2$ is not an integral number of blocks, no such 6-tuple can exist. This proves Lemma (4.9) along with the following corollary:

(4.13) Corollary: Any (16,256,6) code, C , with $\underline{0} \in C$ contains a weight 6 code word, whose complementary vector is also a code word.

(4.14) Lemma: Any (16,256,6) code, C , with $\underline{0} \in C$ contains $\underline{j}$, the all one vector of length 16 .

Proof: Let $\underline{z}$ be a weight 6 code word of C , whose complement $\underline{j} + \underline{z}$ is also a code word, as guaranteed by

Corollary (4.13). Consider $C + \underline{z}$. Not only are $\underline{0}$ and 112 weight 6 code words in $C + \underline{z}$, but $\underline{j} = (\underline{j}+\underline{z})+\underline{z} \in C+\underline{z}$. By Lemma (4.9) all the 112 weight 10 code words are complementary to the 112 weight 6 code words. Since $\underline{z} = \underline{0}+\underline{z}$ is one of the weight 6 code words in $C+\underline{z}$, both $\underline{z}$ and $\underline{j}+\underline{z}$ are code words of $C + \underline{z}$. Therefore $(\underline{j}+\underline{z})+\underline{z} = \underline{j}$ is a code word of C.

(4.15) Corollary: If C is any (16,256,6) code with $\underline{0} \in C$, then the complement of any code word is also a code word of C.

Proof: Let $\underline{w}$ be any code word of C, then $c + \underline{w}$ contains $\underline{0}$ and is a (16,256,6) code. Then, by Lemma (4.4), $\underline{j} \in C+\underline{w}$. Therefore $\underline{w} + \underline{j} \in C$.

(4.16) Theorem: (A restatement of Theorem (4.1)): If C is a (16,256,6) code with $\underline{0} \in C$, then C contains also 112 weight 6 code words, 15 weight 8 code words, no two of which are complementary, together with the vectors complementary to those $1 + 112 + 15 = 128$ code words.

Proof: This is a result of Lemmas (4.2), (4.4) and Corollary (4.15).

(4.17) Corollary: Any (16,256,6) code, C, with $\underline{0} \in C$, has the same weight distribution as any of the coset codes $C + \underline{z}$, for any $\underline{z} \in C$.

Proof: Because $C + \underline{z}$ is also a (16,256,6) code with $0 = \underline{z} + \underline{z} \in C + \underline{z}$, for any $\underline{z} \in C$, Theorem (4.16) applies.

§6.5 Each XNR-Design Builds a (16,256,6) Code in just One Way

To build a (16,256,6) code from an XNR-design, Theorem (4.1) requires that the code be complemented, so the 112 needed weight 10 vectors must form the design complementary to the given design. Then to complete this set of $1+112+112+1$ vectors to a (16,256,6) code, 30 weight 8 vectors must be carefully selected. In trying to establish Theorem (5.2), which says that these can be chosen in only one way relative to a given XNR-design, we shall explore a necessary condition for these "admissible" weight 8 vectors.

(5.1) Define an admissible weight 8 vector to be a weight 8 vector which together with the set of $1+112+112+1$ vectors given by $\underline{0}$, the 112 weight 6 vectors in the given XNR-design and their complements preserve the distance condition $d \geq 6$.

(5.2) Theorem: Given XNR-design, then admissible weight 8 vectors (by Definition (5.1)) are symmetric differences in 28 ways of two weight 6 vectors from D which share two coordinate places.

Proof: Let L be the 8-tuple indicated by an admissible weight 8 vector. By the condition $d \geq 6$, L meets blocks of the XNR-design D in at most 4 places; so $b^L_{5,0} = b^L_{6,0} = b^L_{7,0} = b^L_{8,0} = 0$. Let $b^L_{4,0} = x$, then the $b^L_{i,j}$ become:

(5.3)

$$
\begin{array}{cccccccccc}
 & & & & 112 & & & & & \\
 & & & 70 & & 14 & & & & \\
 & & 42 & & 28 & & 14 & & & \\
 & 24 & & 18 & & 10 & & 4 & & \\
12+x & & 12-x & & 6+x & & 4-x & & x & \\
 & 2+5x & & 10-4x & & 2+3x & & 4-2x & & x \\
 & & -10+15x & & 12-10x & & -2+6x & & 4-3x & \\
 & & & -28+35x & & 18-20x & & -6+10x & & 4-4x \\
 & & & & -56+70x & & 28-35x & & -10+15x & \\
 & & & & & & & & & 4-5x
\end{array}
\qquad
\begin{array}{cccc}
 & & & \\
 & & & \\
 & & & \\
 & & & \\
x & & & \\
 & x & & \\
 & & x & \\
 & & & x \\
 & & & \\
 & & & x
\end{array}
\qquad
\begin{array}{cccc}
 & & & \\
 & & & \\
 & & & \\
 & & & \\
0 & & & \\
 & 0 & & \\
 & & 0 & \\
 & & & 0 \\
 & & & \\
 & & & 0
\end{array}
\qquad
\begin{array}{cccc}
 & & & \\
 & & & \\
 & & & \\
 & & & \\
0 & & & \\
 & 0 & & \\
 & & 0 & \\
 & & & 0 \\
 & & & \\
 & & & 0
\end{array}
\quad .
$$

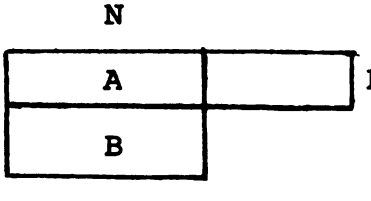
From $-56+70x = b^L_{0,8} \geq 0$ and $4-5x = b^L_{3,5} \geq 0$, we learn that $x = 4/5$, showing that the $b^L_{i,j}$ really are:

(5.4)

$$
\begin{array}{ccccccccc}
 & & & 112 & & & & & \\
 & & 70 & & 42 & & & & \\
 & 42 & & 28 & & 14 & & & \\
24 & & 18 & & 10 & & 4 & & \\
 & 64/5 & & 56/5 & & 34/5 & & 16/5 & 4/5 \\
6 & & 34/5 & & 22/5 & & 12/5 & 4/5 & 0 \\
 & 2 & & 14/5 & & 8/5 & & 4/5 & 0 \\
0 & & 2 & & 4/5 & & 4/5 & 0 & 0 \\
 & 0 & & 2 & & 0 & & 4/5 & 0
\end{array}
$$

From the $b^L_{i,j}$ values with $i + j = |L| = 8$ we can now see that an admissible weight 8 vector meets a weight 6 vector in either 2 or 4 places. But these $b^L_{i,j}$ tell us even more. Let us view the incidence matrix N of the design D as sectioned into two halves, upper and lower, according to the 8-tuple L. Then we have

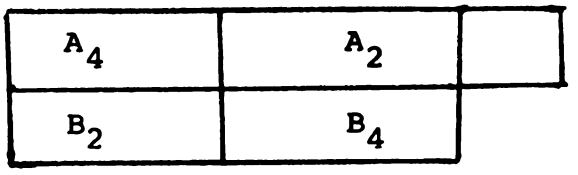
Figure (5.5)



.

Here the $x \times 112$ matrix A represents those parts of the blocks of D meeting L, and B represents those parts missing L. Matrix A can further be divided into two parts according to its parts of blocks of weight 2 and its parts of weight 4. After permuting the blocks so that all the weight 4 parts occur to the left we obtain:

Figure (5.6)



Here $A = [A_4, A_2]$ and A_4 represents a design of weight 4 blocks on the 8 points of L while B_2 represents a design of weight 2 blocks on the other 8 points (which comprise the rest of the blocks of D through A_4.)

Since D is a $4\text{-}(3,6,16)$ design, each 3 points of L must be located in precisely 4 blocks of A. These blocks must be all in A_4, so A_4 is necessarily a $4\text{-}(3,4,8)$ design. Since a $4\text{-}(3,4,8)$ design has $b_2 = 12$ while design D has $b_2 = |L|$, each pair of points from L must occur twice as a block in design A_2. Thus, A_2 actually consists of two copies of the complete pair design from 8 points. Denote A_2 by $[\binom{8}{2}, \binom{8}{2}]$ to indicate that each pair of points from L is a block of A_2 occurring twice. By exactly the same reasoning relative to the other 8 points, not contained in L, B_2 is two copies of the complete $\binom{8}{2}$-design, and B_4 is a $4\text{-}(3,4,8)$ design.

Now we wish to show that the two blocks of B_2

representing any fixed pair of points from the complement L' of L, are attached to complementary, disjoint weight 4 blocks of A_4. Once this is shown, we have the fact that L is necessarily the modulo 2 sum or equivalently the symmetric difference of two weight 6 blocks of D, which meet each other on two places - the fixed pair from L'. In fact, since this must be true relative to any fixed pair of points chosen from L', L is the symmetric difference in 28 ways of two blocks of D, which share two places since $28 = \binom{8}{2}$ is the number of pairs from L'.

It suffices now to fix our attention on a pair of points, say points 1 and 2 from L', the complement of set L. Choose also an arbitrary point, say α, from set L itself.

(5.7) Claim: The sub-design of B_4 corresponding to exactly those blocks of D passing through B_4 and containing point α is a $1-(3,4,8)$ design.

Proof: Consider the design A_2. This design has $b_1 = 14$, so α is contained in 14 blocks of D which pass through B_4. Now consider the design E of the 14 blocks of B_4 on the 8 points of L'. Since blocks of weight 2 in A_2 and all containing α differ in at most one place, such blocks have Hamming distance ≤ 2, when considered as vectors. Yet blocks of D have Hamming distance ≥ 6. So the 14 blocks of E have Hamming distance ≥ 4. Now Lemma (4.7.7), applies with $[\frac{v-t}{k-t}] = \frac{v-t}{k-t}$ so that E is a $1-(3,4,8)$ Steiner system. This proves the Claim (5.7). //

Since by (5.7) E has $b_2 = 3$, the triple of points $\{\alpha,1,2\}$ are contained in precisely three blocks of D passing through A_2. As such, that triple $\{\alpha,1,2\}$ is necessarily contained in a unique $(1 = 4-3)$ block of D passing through A_4.

(5.8) This can be interpreted as: Given the pair $\{1,2\}$ from L', then each point α of L, the triple $\{\alpha,1,2\}$ is contained in a unique block of D and meeting L in four places.

Finally, we notice that there are two blocks of D meeting L' in precisely $\{1,2\}$ and meeting L in four places. By (5.8) the 4-tuple parts of the two blocks of D in question must be disjoint and complementary, relative to L. This proves the theorem. //

(5.9) Theorem: Each XNR-design builds a (16,256,6) code C uniquely.

Proof: According to Theorem (4.1) to form an XNR-design D one must choose the vectors $\underline{0}$, $\underline{j}$, and the 112 complements of the weight 6 vectors indicated by D. Furthermore, by Theorem (5.2) one may choose as admissible weight 8 vectors only those vectors of weight 8 which are symmetric differences of weight 6 vectors meeting one another on precisely two places. By the $b^L_{i,j}$ for a block L of design D, as listed in (4.6), each weight 6 vector meets exactly one other block in each of its $\binom{6}{2} = 15$ pairs; so each weight 6 vector meets 15 other weight 6 vectors in precisely two places.

Choosing the weight 6 vectors in turn gives

$$112.15/2! = 840$$

admissible weight 8 vectors. But again by Theorem (5.2) each of these must be formed as a symmetric difference in 28 ways, so there are but 840/28 = 30 admissible weight 8 vectors possible. By Theorem (4.1), all of these must be used to complete design D to a (16,256,6) code. //

§6.6 Conclusion

Restating the previous Theorem (5.9) in a form more suitable for later use we have:

(6.1) Theorem: The (16,256,6) code is unique (up to a permutation of the 16 points of the design) if the XNR-design is unique.

CHAPTER 7

Coordinatization of the XNR (16,256,6) Code by V(4,2)

§7.1 Introduction

By Theorem (6.6.1), we need only show that the XNR-design is unique in order to conclude the uniqueness of the XNR (16,256,6) code. Proceeding towards this goal we show in this chapter that the vectors of the XNR (16,256,6) code can always be viewed as characteristic functions of dependent sets in V(4,2), Theorem (5.1). Then combining Theorems (6.6.1) and (5.1), it can be seen that any XNR-design is embeddable in V(4,2). This reduces the problem to studying PG(3,2) and V(4,2) in order to see that the design is unique. Chapters 8 and 9 accomplish this latter part of the uniqueness proof.

§7.2 Coherent 4-Tuple Vectors

The concept of coherent 4-tuples is important in the analysis of the design of the weight 8 vectors from the XNR code as well as essential in building the S(4,7,23) design from the XNR-design. Briefly described, the coherent 4-tuples are precisely all those 4-sets not contained in any block of the XNR-design. We shall now define these carefully and show that there are 140 such coherent 4-sets

weight 10 vectors of XNR are precisely the complementary vectors of the weight 6 vectors of XNR (Lemma (6.4.9)), any weight 8 vector meets 56 weight 10 vectors of XNR at distance 6 and the other 56 weight 10 vectors of XNR at distance 10, respectively. Then by the Theorem (6.4.1), any weight 8 vector of XNR must meet other vectors of the set $\mathcal{B}$ of weight 0,8, and 16 vectors of XNR at distance 8 or 16. One now sees that the code $\mathcal{B}$ has minimum distance 8 and contains, for each $\underline{x} \in \mathcal{B}$ a vector also of $\mathcal{B}$ and at distance 16 from $\underline{x}$. This means that the complementary vector $\underline{x}+\underline{j}$ is necessarily in $\mathcal{B}$, and that $\mathcal{B}$ is therefore complemented. //

(3.4) Lemma: The 30 weight 8 vectors of XNR (16,256,6) form the columns of a 3-(3,8,16) complemented design with $d \geq 8$.

Proof: Since the complement of a weight 8 vector is again of weight 8 and since code $\mathcal{B}$ is complemented, the design C corresponding to the weight 8 vectors of XNR is a complemented design.

Considering weight 8 code vectors as 0,1 incidence matrix columns, choose any three of the rows of this 16×30 matrix. Assume that these three rows are contained in at least four blocks, B_1, B_2, B_3, and B_4, where blocks are the sets of cardinality 8 given by the ones from the columns of the matrix. Then

§7.3 The 3-(3,8,16) Design with $d \geq 8$ of the Weight 8 Vectors of XNR (16,256,6) and the Reed-Muller Code $\mathcal{B}$ with Parameters (16,32,8)

(3.1) Given the XNR (16,256,6) code, let $\mathcal{B}$ be the sub-code of weight 0, 8, and 16 vectors. Then $\mathcal{B}$ is a (16,1+30+1,d) code for d to be yet determined. We shall now show, Lemma (3.3), that $d = 8$.

(3.2) $\mathcal{B}$ is referred to in the literature as the first order Reed-Muller code of length 16 (cf. Petersen [30], Berlekamp [3]).

(3.3) Lemma: $\mathcal{B}$ as defined in (3.1) has minimum distance 8, and is a (16,32,8) complemented code (i.e. the complementary vector to each vector of the code is again in the code).

Proof: By Theorem (6.4.1), the XNR code contains 30 vectors of weight 8 and 112 vectors of weight 6 and 10, respectively. Considering the 6-sets and 8-sets for which the weight 6 and 8 code vectors are characteristic functions, we see from the generalized block intersection numbers for the XNR-design $\mathcal{B}$ of those 6-sets relative to a given 8-set L (cf. (6.5.4)) that L meets 6-sets either in two or four places. Moreover, L meets precisely $2.\binom{8}{2} = 56$ of the 6-sets in two places and $\frac{4}{5}.\binom{8}{4} = 56$ of them in four places. Translated into terms of vectors, any weight 8 vector of XNR meets 56 weight 6 vectors of XNR at distance 10 and the other 56 weight 6 vectors of XNR at distance 6. Since the

which together form a S(3,4,16) design.

(2.1) Let D be the XNR-design. Since $d \geq 6$, $b^{L}_{4,0}$ is equal to 1 for any block L of the design (cf. (6.4.6)). In other words, each 4-set from the set of 16 points is contained either in one unique block of D or not at all.

(2) Define a 4-set to be a <u>coherent 4-tuple</u> relative to D if the 4-set is contained in no block of D. A <u>coherent 4-tuple vector</u> is then the characteristic function vector of a coherent 4-tuple.

(2.3) <u>Lemma</u>: The coherent 4-tuples relative to the given XNR-design D form a 1-(3,4,16) or S(3,4,16) Steiner system. There are 140 such coherent 4-tuples.

<u>Proof</u>: Since each 4-tuple of D, cf. (2.1), is contained in at most one block of D, there are $\binom{16}{4}-112\binom{6}{4} = 140$ coherent tuples. Any 3-tuple is contained in four blocks of D, say $A_i, i = 1,2,3,4$. Since $|\bigcup_{i=1}^{4} A_i| = 15$, the 3-tuple plus the remaining $16^{\underline{th}}$ point form a 4-tuple, which is contained in no block of D (since the four blocks, A_i, are the only blocks containing the 3-tuple). Thus each 3-tuple is in at least one coherent 4-tuple. But an average indicates

$$\hat{b}_3 = \frac{140.\binom{4}{3}}{\binom{16}{3}} = 1 .$$

Thus, the 4-tuples form a 1-(3,4,16) design. //

$$\left|\bigcup_{i=1}^{4} B_i\right| = \sum_{i=1}^{4} |B_i| - \sum_{i\neq j} |B_i \cap B_j| +$$

$$\sum_{i\neq j\neq k\neq i} |B_i \cap B_j \cap B_k| - \left|\bigcap_{i=1}^{4} B_i\right|$$

$$= 4.8 - 6.4 + \Sigma|B_i \cap B_j \cap B_k| - \left|\bigcap_{i=1}^{4} B_i\right| .$$

Since $|B_i \cap B_j \cap B_k| = 3$ or 4, $|\cup B_i| \geq 17$, a contradiction. Therefore no 3-tuple of rows is contained in more than 3 blocks. However,

$$\hat{b}_3 = \frac{30.\binom{8}{3}}{\binom{16}{3}} = 3, \quad \text{from (4.1.8)} .$$

Thus $b_3 = 3$ and the design C is a 3-(3,8,16) design. Finally, since these weight 8 vectors are all contained in code $\mathcal{B}$ with minimum distance 8, C is a 3-(3,8,16) design with $d \geq 8$. //

§7.4 The Linearity and Uniqueness of the Reed-Muller (16,32,8) Code $\mathcal{B}$ Contained in XNR (16,256,6)

As a consolidation of the Lemmas (4.3) and (4.4) in this section we prove:

(4.1) Theorem: The (16,32,8) code $\mathcal{B}$ formed by the weight 0, 8, and 16 vectors of a (16,256,6) XNR code is linear and unique up to a permutation of the 16 coordinates.

(4.2) Lemma: For C being the 3-(3,8,16) design with $d \geq 8$ corresponding to the weight 8 vectors in XNR, any three points of the design are contained in a unique

coherent 4-tuple which is in turn contained in precisely three blocks of C .

Proof: Choose any weight 8 block B . Choose any three rows incident with B . There are four weight 6 blocks, A_1, A_2, A_3, and A_4 , incident with these three rows. Each of these A_i meets B in exactly 4 places, because the corresponding weight 6 code vectors meet the weight 8 code vector in either 2 or 4 places.

This gives

$$|(\bigcup_{i=1}^{4} A_i) \cap B| = 7 .$$

Therefore, the $8^{\underline{th}}$ row incident with B together with those 3 rows form a coherent 4-tuple of rows. Furthermore, all of these four rows are incident with B .//

(4.3) Lemma: $\mathcal{B}$ is a linear code.

Proof: Consider any two vectors $\underline{z}_1$ and $\underline{z}_2$ in $\mathcal{B}$. If either of these is $\underline{0}$ or $\underline{j}$, or if these vectors are complementary, then their sum is also in $\mathcal{B}$, since $\mathcal{B}$ is a complemented code.

Let $\underline{z}_1$ and $\underline{z}_2$ correspond to two non-complementary weight 8 blocks, B_1 and B_2 . Since $\underline{z}_1$ and $\underline{z}_2$ are at distance 8, $|B_1 \cap B_2| = 4$. Now considering any triple of rows incident with $B_1 \cap B_2$, one can see that $B_1 \cap B_2$ is a coherent 4-tuple by Lemma (4.2). But furthermore, the three rows are incident with also a third block B_3 of the 3-(3,8,16) design with $d \geq 8$. Therefore

$$B_1 \cap B_2 \cap B_3 = B_1 \cap B_2 = B_1 \cap B_3 = B_2 \cap B_3 .$$

Let $\underline{z}_3$ be the weight 8 code vector corresponding to B_3. Then $\underline{z}_1 + z_2 = \underline{j} + \underline{z}_3$ which is in $\mathcal{B}$. Hence, $\mathcal{B}$ is linear. //

(4.4) Lemma: Up to a permutation of the 16 basis coordinate positions of $V(16,2)$, the code $\mathcal{B}$ is unique.

Proof: Since $\mathcal{B}$ is linear, $\mathcal{B}$ can be linearly generated by a 5×16 matrix G, where the rows of G are five linearly independent vectors from D. Choose such a basis so that $\underline{j}$ is the first row of G and so that $\underline{z}_i, i = 1,2,3,4,$ are the other basis vectors. Let B_i, $i = 1,2,3,4$, be the weight 8 blocks corresponding to the $\underline{z}_i$, $i = 1,2,3,4$. Since $\underline{j}$ is a basis vector

(4.5) $|B_i \cap B_j| = 4 \quad i \neq j, \ i, j = 1,2,3,4$.

If $|B_i \cap B_j \cap B_k| \geq 3$ for distance $i,j,k \in \{1,2,3,4\}$, then Lemma (4.2) implies that $|B_i \cap B_j \cap B_k| = 4$, so that $\underline{z}_i + \underline{z}_j = \underline{j} + \underline{z}_k$. This contradicts the linear independence of those four vectors.

If $|B_i \cap B_j \cap B_k| = 0$, then $\underline{z}_i + \underline{z}_j = \underline{z}_k$, again a contradiction.

If $|B_i \cap B_j \cap B_k| = 1$, then the distance between $\underline{z}_i + \underline{z}_j$ and z_k is 4, contradicting the fact that the linear code $\mathcal{B}$ has distance $d \geq 8$, Lemma (3.3).

Hence

(4.6) $|B_i \cap B_j \cap B_k| = 2, i \neq j \neq k \neq i; \ i,j,k \in \{1,2,3,4\}$.

If $|\bigcap_{i=1}^{4} B_i| = 2$, then $\underline{z}_1 + \underline{z}_2 + \underline{z}_3 = \underline{z}_4$.

If $|\bigcap_{i=1}^{4} B_i| = 0$, then $\underline{z}_1 + \underline{z}_2 + \underline{z}_3 = \underline{j} + \underline{z}_4$. Thus we

conclude

$$(4.7) \qquad \Big|\bigcap_{i=1}^{4} B_i\Big| = 1 \ .$$

Statements (4.5), (4.6), and (4.7) applied in reverse order show that, up to a permutation of the 16 columns, the last four rows of G are:

$$(4.8) \qquad G^* = \begin{bmatrix} 1&1&1&1&0&1&1&1&0&0&0&1&0&0&0&0 \\ 1&1&1&0&1&1&0&0&1&1&0&0&1&0&0&0 \\ 1&1&0&1&1&0&1&0&1&0&1&0&0&1&0&0 \\ 1&0&1&1&1&0&0&1&0&1&1&0&0&0&1&0 \end{bmatrix} \ .$$

Hence,

$$(4.9) \qquad G = \begin{bmatrix} \mathbf{j} \\ G^* \end{bmatrix} \ .$$

Since $\mathbf{j}$ is always in the linear code $\mathcal{B}$, there is no loss in generality in assuming that $\mathbf{j}$ is also in the generator matrix G for $\mathcal{B}$. Consequently, up to a permutation of the 16 standard basis vectors for $V(16,2)$, the $(16,32,8)$ code $\mathcal{B}$ is unique. //

§7.5 Coordinatization of XNR by Points of V(4,2)

(5.1) Theorem: There exists an isomorphism:

$$\alpha : V(16,2) \to 2^{V(4,2)}$$

so that α maps the standard basis vectors of $V(16,2)$ to the points of $V(4,2)$ and so that each of the code vectors in XNR $(16,256,6)$ become characteristic functions of

linearly dependent sets in $V(4,2)$.

This theorem shall be proved by Lemmas (5.4) and (5.8) which tell more than what appears in the statement of Theorem (5.1). In particular these lemmas show that the XNR code contains the Reed-Muller first order code of length 16 and is contained in the extended Hamming code of the same length. The other lemmas in this section describe in detail the nature of the linear dependent sets in question.

(5.2) Let G be a generator matrix for the linear $(16,32,8)$ code $\mathcal{B}$ as given in (4.9). Then define a code $\mathcal{S}$ to be the orthogonal code to $\mathcal{B}$ in $V(16,2)$:

(5.3) $\underline{x} \in \mathcal{S} \Leftrightarrow G\underline{x} = \underline{0}$.

(5.4) Lemma: $\mathcal{S} \supset XNR \supset \mathcal{B}$.

Proof: That $XNR \supset \mathcal{B}$ is by definition. $\mathcal{S}$ depends only on $\mathcal{B}$, not on all of XNR, and, in fact, $\mathcal{S}$ is the orthogonal space to $\mathcal{B}$ in $V(16,2)$. Since each weight 8 vector of XNR meets weight 6 and 10 code words of XNR in an even number of places, and meets other weight 8 code words in an even number of places, $\mathcal{B}$ is orthogonal to XNR . Hence $\mathcal{S} \supset XNR$. //

We now define the mapping α needed for Theorem (5.1).

Let G^* be the matrix G less the row $\underline{j}$. Then as in (4.8), up to a permutation $\varphi \in S_{16}$, the symmetric group of all permutations of the 16 standard basis vectors of $V(16,2)$, G^*, can be given as:

(5.5)
$$G^* = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}$$

For the matrices G and G^* as given above, define the one to one correspondence:

(5.6) $\alpha : \underline{e}_i \to \alpha(\underline{e}_i) = \{\underline{p}_i\} \subset V(4,2)$

where $\underline{e}_i = (0,0,\ldots,1,0,\ldots,0)$, the basis vector of $V(16,2)$ with a single one in the $i^{\underline{th}}$ place, and where $\underline{p}_i$ is the $i^{\underline{th}}$ column of G^*. Now extend this definition linearly to all vectors of $V(16,2)$ by

(5.7) $$\alpha\left(\sum_{i=1}^{16} x_i \underline{e}_i\right) = \cup\{\underline{p}_i \mid x_i = 1\} .$$

For example, $\alpha(\underline{e}_1 + \underline{e}_2) = \{\underline{p}_1, \underline{p}_2\}$. Thus, α is a well-defined linear map of $V(16,2)$ onto $2^{V(4,2)}$.

(5.8) <u>Lemma</u>: $\mathcal{g}$ is the Extended Hamming code $\overline{C}_4$ of length 16.

<u>Proof</u>: Define the subsequent map: $\beta : 2^{V(4,2)} \to V(4,2)$ by

$$\beta(\cup\{\underline{p}_i\}) = \Sigma \underline{p}_i = \underline{p}_j \in V(4,2), \quad i,j = 0,1,2,\ldots,15 .$$

Then $\beta\circ\alpha$, the composition of first α and then β, is a linear homomorphism of $V(16,2)$ onto $V(4,2)$ so that

(5.10) $(\beta\circ\alpha)\underline{x} = G^*\underline{x}$.

It follows from the fact that G^* is the matrix G less the row containing j and the definition of $\mathcal{g}$, (5.3), that $\mathcal{g} \subset (\beta\circ\alpha)^{-1}(\underline{0})$. Therefore all vectors of $\mathcal{g}$ are characteristic functions of dependent sets in $V(4,2)$.

But moreover since vectors of δ are also orthogonal to j as well as merely G^*, the entry in the p_0 coordinate place is either 1 or 0 so as to make the weight of the entire vector even. So combining Lemma (2.6.3) with this last statement, δ is necessarily the parity check code $\overline{C}_4$ of the Hamming C_4 of length 15. //

For the rest of this section assume that the map α is defined as in (5.6) and (5.7) and is that described in Theorem (5.1).

(5.11) Lemma: The weight 6 vectors of XNR are the characteristic functions of 112 of the 448 possible dependent 6-sets in V(4,2). These dependent 6-sets are symmetric sums of pairs of planar 4-sets in V(4,2) which span all of V(4,2) and which intersect in one point.

Proof: We have seen in Lemma (5.3.3) that there are 448 dependent 6-sets in V(4,2). Since by Lemma (5.4) and Theorem (5.1), XNR $\subset \overline{C}_4$, all the weight 6 vectors of XNR correspond to some (in fact 112) of the possible dependent 6-sets in V(4,2).

Let a typical dependent 6-set be $\{\underline{x}_1, \underline{x}_2, \underline{x}_3, \underline{x}_4, \underline{x}_5, \underline{x}_6\}, L$. Choose any three of these, say $\{\underline{x}_1, \underline{x}_2, \underline{x}_3\} = M$. Then there is a unique fourth point $\underline{x}_7$ from V(4,2) so that $M \cup \{\underline{x}_7\}$ is a dependent 4-set in V(4,2). Note that $\underline{x}_7$ is not already in L since a dependent 6-set by Lemma (4.5.8) was shown to have no four of its points in a plane. If $\underline{x}_8$ is the unique point completing $L \setminus M$ to a plane then

set union $((L \setminus M) \cup \{\underline{x}_8\}) \cup (M \cup \{\underline{x}_7\}) = \{\underline{x}_i \mid i = 1,\ldots,8\}$ is also dependent. Then the symmetric difference $L \Delta \{x_i \mid i = 1,\ldots 8\} = \{x_7, x_8\}$ is also dependent. Then the symmetric difference $L \Delta \{\underline{x}_i \mid i = 2,\ldots,8\} = \{\underline{x}_7, \underline{x}_8\}$ is again dependent showing that $\underline{x}_8 = \underline{x}_7$. In this way, L is the symmetric difference of two planar 4-sets sharing one point. Finally these two planar 4-sets span V(4,2) because their union contains L which spans V(4,2) by Lemma (4.5.8). //

(5.12) Lemma: Under α , coherent 4-tuple vectors defined from the weight 6 vectors of XNR (cf. Definition (2.2)) are the characteristic vectors of all the 140 planar 4-sets in V(4,2) .

Proof: Let L be any 8-set of V(16,2) corresponding to a weight 8 vector of XNR , and let C be the 3-(3,8,16) design with $d \geq 8$ of all such 8-sets. Let B be any coherent 4-tuple. Viewing the generalized block intersection numbers $b^B_{i,j}$ for the design C relative to the coherent 4-tuple B we have:

(5.13)

				30				
			15		15			
		7		8		7		
	3		4		4		3	
x		3-x		4+x		3-x		x

where $b^B_{4,0} = x$. By Lemma (4.2), if any three points of B are contained in L , $B \subset L$, we have $b^B_{3,1} = 0 = 3-x$ so that $x = 3$. Consequently $b^0_{1,3} = 0$ and B meets every block of C in an even number of places. Therefore for

every coherent 4-tuple vector $\underline{v} \in V(16,2)$, $\underline{v}$ is orthogonal to the code $\mathcal{B}$ of all weight 0,8, and 16 vectors of XNR. Hence, $\underline{v} \in \mathcal{S} = \overline{C}_4$ by Lemma (5.8) and $\underline{v}$ is a characteristic vector of a dependent 4-set or planar 4-tuple in V(4,2) by Theorem (5.1). Since there are 140 coherent 4-tuples and the same number of planar 4-sets in V(4,2), α identifies these sets. //

(5.14) Lemma: Under α, weight 8 vectors of XNR are characteristic functions of the 30 copies of V(3,2) in V(4,2).

Proof: Again using Lemma (4.2) we shall see that if three points of V(4,2) of a planar 4-set are contained in the image 8-set under α of a weight 8 code word in XNR, then all four points of that planar 4-set are contained in that 8-set. This implies that each 8-set arising in this way is the linear span of its points. Since any 8-set in V(4,2) contains four independent points, the span of these is a V(3,2) which must coincide with the 8-set. There are 30 copies of V(3,2) in V(4,2), so α identifies these sets. //

(5.15) Theorem: The stabilizer group of $\mathcal{B}$ in S_{16} (the symmetric group of all permutations of the 16 coordinates of V(16,2)) is a degree 16 representation of Aut(V(4,2)).

Proof: Let $\gamma = \beta \circ \alpha : V(16,2) \to V(4,2)$ for α as in (5.6) and (5.7) and for β as in (5.9) be the linear homomorphism given by

$$\gamma(\underline{x}) = (\beta \circ \alpha)(\underline{x}) = G^* \underline{x}$$

with α,β, and G^* as in (5.5) . $\mathrm{Aut}(V(4,2))$ is the set of motions ψ of $V(4,2)$ preserving linear dependency. Thus, for each $\psi \in \mathrm{Aut}(V(4,2))$, $\gamma^{-1}\psi \in S_{16}$ and γ^{-1} stabilizes $\mathcal{G}$. Since $\gamma^{-1}\psi(G^*) = G^*$ only if $\psi = 1$, the group $\mathcal{L} \subset S_{16}$ which stabilizes $\mathcal{G}$ has no more elements then the number of distinct generator matrices

$$G = \begin{bmatrix} j \\ \\ G^* \end{bmatrix} \text{ for } \mathcal{B} .$$

This number is $30.28.24.16$, since that is the number of ways of choosing 4 linearly independent vectors of $\mathcal{B}$ that together with j form a basis of $\mathcal{B}$. Consequently,

$$|\mathcal{L}| \leq 30.28.24.16 .$$

But $\mathcal{L}$ contains a subgroup isomorphic to $\mathrm{Aut}(V(4,2))$ which has the same order. Hence $\mathcal{L} \simeq \mathrm{Aut}(V(4,2))$. //

CHAPTER 8

Coordinates for Lines of PG(3,2)

§8.1 Introduction

In order to show the uniqueness in Theorem (9.5.1) of the XNR-design within the context of V(4,2) and PG(3,2), we need to use the fact that the alternating group A_7 operates transitively on the 35 lines of PG(3,2). Therefore we shall establish in this chapter the classical isomorphism $PLS(4,2) \simeq A_8$ and determine eight coordinates for lines of PG(3,2) .

The classical isomorphism making possible the needed coordinatization was early known to group theorists, (cf. Dickson [13], and as early as 1910 was interpreted in a geometrical context by Conwell [10]. Perhaps this geometrical representation was forgotten, for the same sort of work was duplicated by Edge [14] in 1954 and just recently duplicated independently (for different goals) by Jonsson in [19] and Seidel in [5] and [6].

A seven coordinate system for lines of PG(3,2) was introduced by Gleason in a very efficient manner in 1952 (cf. Wagner [38]). This development would suffice for our purposes, but we shall instead develop these coordinates in

a new manner which will lend a bit more insight into the geometric counterparts of these seven and eight coordinates for lines of PG(3,2).

§8.2 Finding PG(5,2) within V(8,2)

(2.1) Given V(8,2), consider the set of all even weight vectors. These form a V(7,2) within V(8,2), in fact, the hyperplane $\sum_{i=1}^{8} \underline{x}_i = 0$.

(2.2) Define a relation "$\sim$" by

$\underline{x} \sim \underline{y}$ if $\underline{y} = \underline{x}$ or $\underline{y} = \underline{x} + \underline{j}$, where $\underline{j}$ is the all-one column vector of length 8.

(2.3) This relation is easily seen to be an equivalence relation. Now define "+" and "." for these equivalence classes:

(2.4) $\langle \underline{x} \rangle + \langle \underline{y} \rangle := \langle \underline{x} + \underline{y} \rangle \quad \underline{x}, \underline{y} \in V(7,2)$

(2.5) $\lambda \langle \underline{x} \rangle := \langle \lambda \underline{x} \rangle \quad \underline{x} \in V(7,2), \ \lambda \in GF(2)$.

Now it is clear that the set of equivalence classes under $\sim$ of V(7,2) with the "+" and "." operations defined in (2.4) and (2.5) form a V(6,2).

(2.6) Finally by restricting our attention to the vector equivalence classes other than $\langle \underline{0} \rangle$ we have a copy of PG(5,2) contained in V(8,2).

Remark: This relatively strange way of locating PG(5,2) within V(8,2) is contrived so that we can within this setting show $PSL(4,2) \simeq A_8$.

§8.3 The Klein Quadric

The 128 vectors in $V(7,2)$ considered in (2.1) have length 8. There are $\binom{8}{4} = 70$ weight 4 vectors, $\binom{8}{2} = 28$ weight 2 and weight 6 vectors, plus the $\underline{0}$ and $\underline{j}$ vectors.

It is convenient to subdivide these by

$$(3.1) \qquad \Omega(\underline{x}) = \sum_{i<j}^{8} x_i x_j = 0 \quad \text{where} \quad \underline{x} = (x_1, x_2, \ldots, x_8) .$$

Then vectors of weights 0,4, and 8 have $\Omega(\underline{x}) = 0$ and the others have $\Omega(\underline{x}) = 1$.

The quadratic form Ω has the property that

$$(3.2) \qquad \Omega(\underline{x}) = 0 \text{ iff } \Omega(\underline{j} + \underline{x}) = 0 \quad \text{for} \quad \underline{x} \in V(7,2) .$$

Because of this, Ω is well defined on equivalence classes, $<\underline{x}>$, under $\sim$ as defined in (2.2). Thus, choosing representative vectors of these equivalence classes to be of weights 2 and 4 we see that in $PG(5,2)$ (cf. (2.6)):

$$(3.3) \qquad \Omega(<\underline{x}>) = 1 \text{ iff } \underline{x} \text{ has weight } 2 ,$$
$$\Omega(<\underline{x}>) = 0 \text{ iff } \underline{x} \text{ has weight } 4 .$$

We can relate the quadratic form Ω given in (3.1) to the Klein quadric (cf. [1] or [35]) in $PG(5,2)$ as follows.

Under the transformation:

$$(3.4) \qquad y_1 = x_3 + x_5 + x_8 , \; y_5 = x_2 + x_3 + x_8$$
$$y_2 = x_4 + x_6 + x_8 , \; y_6 = x_1 + x_4 + x_7$$
$$y_3 = x_2 + x_6 + x_7 , \; y_7 = x_2 + x_4 + x_5$$
$$y_4 = x_1 + x_5 + x_8 , \; y_8 = x_1 + x_3 + x_6$$

(3.5) $\sum_{i<j}^{8} x_i x_j = y_1y_2 + y_3y_4 + y_5y_6 + y_7y_8$

showing that Ω is a hyperbolic quadric (cf. [1] or [35]) in $V(8,2)$. This transformation maps even weight vectors onto even weight vectors and the all one vector onto itself.

Then by considering the equivalence classes under $\sim$ (in (2.2)), one may set

(3.6) $y_8 = 0$

and see that $\Omega = 0$ corresponds to

(3.7) $y_1y_2 + y_3y_4 + y_5y_6 = 0$ in $PG(5,2)$.

This statement (3.7) is equivalent to E. Artin's definition of the Klein quadric in $PG(5,q)$ for $q = 2$, cf. [1] . Therefore we may define:

(3.8) K = the Klein quadric = $\{\langle x\rangle \in PG(5,2) \mid \Omega(\langle \underline{x}\rangle) = 0\}$

or equivalently, due to (3.3).

(3.9) K = the Klein quadric = $\{\langle \underline{x}\rangle \in PG(5,2) \mid |\underline{x}| = 4\}$.

§8.4 Graph Theory Definitions

(4.1) A graph is a pair (X,E), where X is a set of elements called vertices, and E is a set of pairs of elements from X called edges.

(4.2) The edges determine an adjacency relation, so that two vertices, v_1, v_2, of (X,E) are adjacent iff the pair $\{v_1,v_2\}$ is an edge.

(4.3) A graph is connected if there exists a finite sequence of edges of the form $\{\{v_1,v_2\},\{v_2,v_3\},\ldots,\{v_{n-1},v_n\}\}$ for each pair of vertices v_1 and v_n in (X,E) .

(4.4) A complete graph is a graph whose edge set contains all pairs of vertices.

(4.5) A clique in a graph (X,E) is a complete sub-graph.

(4.6) A maximal clique in a graph (X,E) is a clique which cannot be augmented by another vertex and remain a clique.

§8.5 The Graphs G and H and their Maximal Cliques

In our representation of $PG(5,2)$ within $V(8,2)$ given by (2.6), we have the Klein quadric, K, given in (3.8). On K and off K we may define two graphs G and H as follows:

(5.1) Let $G = (X_G, E_G)$ be the graph whose vertices are the 35 points of K and whose edges are given by the adjacency relation:

$$\langle \underline{x} \rangle \text{ is adjacent to } \langle \underline{y} \rangle \text{ iff } \Omega(\langle \underline{x} + \underline{y} \rangle) = 0$$
$$\text{for all } \langle \underline{x} \rangle \text{ and } \langle \underline{y} \rangle \text{ on } K .$$

(i.e. for all $\langle \underline{x} \rangle$ and $\langle \underline{y} \rangle$ so that $\Omega(\langle \underline{x} \rangle) = \Omega(\langle \underline{y} \rangle) = 0$.)

(5.2) Let H be the graph $H = (X_H, E_H)$ whose vertices are the 28 points of $PG(5,2)$ of K, i.e. those $\langle \underline{x} \rangle$ of $PG(5,2)$ so that $\Omega(\langle \underline{x} \rangle) = 1$, and whose edges are given by the adjacency relation:

$$\langle \underline{x} \rangle \text{ is adjacent to } \langle \underline{y} \rangle \text{ iff } \Omega(\langle \underline{x} + \underline{y} \rangle) = 1$$
$$\text{for all } \langle \underline{x} \rangle \text{ and } \langle \underline{y} \rangle \text{ so that } \Omega(\langle \underline{x} \rangle) = \Omega(\langle \underline{y} \rangle) = 1 .$$

Then choosing representatives of the equivalence classes, $\langle \underline{x} \rangle$, to be weight 2 or 4 vectors of $V(8,2)$, as in (3.3) we see that equivalent definitions of the adjacencies for G and H can be given as:

(5.3) $\langle \underline{x} \rangle$ is adjacent to $\langle \underline{y} \rangle$ in G iff $\langle \underline{x}+\underline{y} \rangle$ is also of weight 4 (as both $\langle \underline{x} \rangle$ and $\langle \underline{y} \rangle$ are),

(5.4) $\langle \underline{x} \rangle$ is adjacent to $\langle \underline{y} \rangle$ in H iff $\langle \underline{x}+\underline{y} \rangle$ is also of weight 2 (as both $\langle \underline{x} \rangle$ and $\langle \underline{y} \rangle$ are).

Consider now cliques in G. These by Definitions (3.9), (5.1), and (5.3) are sets T of equivalence classes of complementary weight 4 vectors in $V(8,2)$ with mutual Hamming distance exactly equal to 4. By Lemmas (4.7.7) and (4.7.8) such a set T is a $S(3,4,8)$ whose 7 sets of complementary weight 4 vectors form a clique in G which is maximal, by Lemma (4.7.6). Thus, we have:

(5.5) Lemma: Maximal cliques in G are precisely all the sets of 7 points of the Klein quadric K (cf. (3.8)) in $PG(5,2)$ so that their 14 vector representatives from $V(8,2)$ form all the distinct $S(3,4,8)$ designs T in $V(8,2)$.

Maximal cliques in H are easier to handle. Vertices of H are equivalence classes of complementary pairs of vectors of weight 2 and 6 in $V(8,2)$, by (3.3). Furthermore, two such classes are adjacent iff their weight 2 representative vectors share preciesly one coordinate with entry 1 from $GF(2)$, by (5.2) and (5.4). Then considering simply the combinatorics of choosing representative vectors in a

maximal clique one obtains:

(5.6) Lemma: Maximal cliques in H are of two types:

Type 1: three vectors whose vector sum is $<\underline{0}>$

Type 2: seven vectors no three of which sum up to $<\underline{0}>$.

Proof: If a third vector in the clique is the vector sum in V(6,2) of two others in the clique, then the maximal clique of Type 1, containing these three vectors, is simply this set of three.

If no vector of the clique is the vector sum of any two of the others in the clique, then all vectors of the clique of Type 2 must, in the V(8,2) representation, share a fixed coordinate with value 1. Since there are 7 other coordinates possible for the second coordinate with value 1 for the weight 2 representative, such maximal cliques have 7 vectors. //

(5.7) From the vector sum definition of linearity in V(6,2), $<\underline{x}>$, $<\underline{y}>$, and $<\underline{z}>$ are collinear iff $<\underline{x}>+<\underline{y}>+<\underline{z}> = <\underline{0}>$ and iff $<\underline{z}> = <\underline{x}>+<\underline{y}> = <\underline{x}+\underline{y}>$ (by (2.4)). This leads to geometric interpretations of maximal cliques in G and H:

(5.8) Lemma: Maximal cliques in G correspond to coplanar sets of seven points all contained in the Klein quadric K . Maximal cliques of H of types 1 and 2 correspond respectively to lines completely disjoint from K and to sets of seven points not on K which form a simplex in V(6,2) .

Proof: By (5.7) and (5.1), maximal cliques in G are the linear spans in PG(5,2) of the 7 points; hence, the points must form a Fano plane completely contained on the Klein quadric K .

By (5.6) and (5.7) each Type 1 maximal clique in H is a line of PG(5,2) disjoint from K while Type 2 maximal clique is a set of seven points off K , no three of which are collinear, no four coplanar, no five in a V(3,2), no six in a V(4,2); i.e. a simplex. //

§8.6 $S_8 \simeq Aut(G) \simeq \overline{O}_6(+,2) \simeq Aut(H)$

In the setting of $PG(5,2 \subseteq V(8,2)$ given in Section 8.2, it is particularly easy to establish the isomorphic action of S_8 , the symmetric group of all permutations of the 8 coordinate places of V(8,2), with $\overline{O}_6(+,2)$, the group of all motions of PSL(6,2) stabilizing the Klein quadric. The following series of lemmas will complse Theorem (6.4) which says that $S_8 \simeq Aut(G) \simeq \overline{O}_6(+,2) \simeq Aut(H)$ for graphs G and H as defined in (5.1) and (5.2), and for the Klein quadric defined in (3.8).

(6.1) Lemma: If $\varphi \in S_8$ fixes each vector of V(8,2) of a given weight class $k \neq 0, 8$, then φ is the identity permutation of S_8 .

Proof: Let R be the set of all weight k vectors of V(8,2). Since all weight k vectors are present, it is possible to find a pair of weight k vectors agreeing on all but two coordinate places, and this coordinate pair may be

arbitrarily chosen. Since φ fixes all weight k vectors, φ fixes all weight 2 vectors, and the problem reduces to the case where $k = 2$. Let S be the set of all weight 2 vectors in $V(8,2)$. Because in S one can find a pair of weight 2 vectors sharing precisely one coordinate with value 1 and disagreeing on any given pair of other coordinate places and because φ stabilizes each pair of coordinate places, φ must fix each of the coordinates of that pair. Hence $\varphi = 1 \in S_8$. //

(6.2) Lemma: S_8 is isomorphic to a subgroup of $PSL(6,2)$ which fixes the Klein quadric (defined in (3.8)), hence $S_8 \subset \overline{O}_6(+,2)$.

Proof: For any $\varphi \in S_8$, φ fixes $\underline{0}$ and $\underline{1}$. Since $\underline{1}$ is fixed, φ operates in a well-defined fashion on complementary pairs of vectors of $V(8,2)$. Since $\underline{0}$ is fixed, φ operates on $PG(5,2)$ and so $S_8 \subseteq PSL(6,2)$. Furthermore, φ stabilizes the sets of weight 2 and weight 4 vectors which are representatives of the equivalence classes which are points of $PG(5,2)$ and that set of weight 4 classes is precisely the Klein quadric K as defined in (3.7). So $\varphi \in \overline{O}_6(+,2)$, the stabilizer group within $PSL(6,2)$ of K. Finally, this representation of S_8 within $\overline{O}_6(+,2)$ is faithful if φ fixes all points of $PG(5,2)$, φ fixes all the points not on K, i.e. fixes the weight 2 vectors of $V(8,2)$. Then by Lemma (6.1), $\varphi = 1 \in S_8$. //

(6.3) Lemma: S_8 operates faithfully as a subgroup of each of the groups $Aut(G)$ and $Aut(H)$, where the graphs G and H are defined in (5.1) and (5.2).

Proof: Any $\varphi \in S_8$ preserves linearity of $V(8,2)$ and fixes $\underline{0}$ and $\underline{j}$. Therefore, by Lemma (6.2), φ preserves linearity in $PG(5,2)$. Since φ also stabilizes each weight class of vectors in $V(8,2)$, φ then preserves the adjacencies in graphs G and H according to (5.3) and (5.4). The proof follows by applying Lemma (6.1) and the fact that vertices of G and H correspond respectively to weight 4 and weight 2 vectors. (For the graph G it is important, in order to use Lemma (6.1), that all 70 weight 4 vectors must be fixed. But if 35 representative weight 4 vectors are fixed, the fact that $\underline{j}$ is fixed assures us that the complementary 35 weight 4 vectors are also fixed. //

(6.4) Theorem: $S_8 \simeq \mathrm{Aut}(G) \simeq \overline{O}_6(+,2) \simeq \mathrm{Aut}(H)$.

Proof: By Lemmas (6.2) and (6.3) we have the faithful injection of S_8 into each of these groups. Each non-adjacent pair of vertices in G determines by linearity in $PG(5,2)$ a unique point not on K with a representative weight 2 vector from $V(8,2)$. So each motion $\varphi \in \mathrm{Aut}(G)$ induces a unique motion of $\overline{O}_6(+,2) \subseteq PSL(6,2)$, which agrees with φ on G and preserves linearity. Similarly, since any two non-adjacent vertices in H determine by linearity a unique vector of weight 4 in $V(8,2)$ and hence a unique point of $PG(5,2)$, each $\varphi \in \mathrm{Aut}\, H$ induces a unique motion $\overline{O}_6(+,2) \subset PSL(6,2)$ agreeing with φ on H and preserving linearity. If ρ is any motion of $\overline{O}_6(+,2)$, then ρ in turn induces a unique motion of $V(8,2)$ preserving linearity, stabilizing complementary pairs of

vectors of $V(8,2)$ and fixing $\underline{0}$ and $\underline{j}$. Hence we can inject each of the groups $Aut(G)$, $Aut(H)$, and $\bar{O}_6(+,2)$ into S_8. Finally, these injections are faithful, completing the proof. //

Used in the proof is the following fact that will later be referred to:

(6.5) Corollary: Each $\varphi \in Aut(G)$ extends to a unique motion φ^* of A_8 which stabilizes $\underline{0}, \underline{j}$, equivalence classes of complementary pairs of vectors in $V(8,2)$ and preserves linearity.

§8.7 S_8 is 1-Transitive and A_8 is $\frac{1}{2}$-Transitive on the 30 Maximal Cliques of Graph G

It is well known that the Fano plane, $PG(2,2)$ of 7 points and 7 lines, is combinatorially unique and has an automorphism group of order 168 (cf. [8]). This means that regardless of the numbering of the points of the plane, any two such planes are isomorphic.. Allowing S_7 to operate on these 7 points produce $7!/168 = 30$ distinct but isomorphic numbering schemes. The fact that these are isomorphic can be restated as the fact that S_7 operates on the set of 30 distinct numberings of Fano planes giving one orbit. The most succinct development of this fact is given by Wagner [38].

Rather than quoting the literature, we shall prove the needed result in the context of coding theory.

(7.1) Lemma: Given any $S(3,4,8)$ design T, then its 14 vectors from $V(8,2)$ together with $\underline{0}$ and $\underline{j}$ form a linear $(8,16,4)$ code.

Proof: Since for any $S(3,4,8)$ design each triple occurs in exactly one block, two blocks share at most two places and have Hamming distance ≥ 4. Augmenting the 14 vectors of T by $\underline{0}$ and $\underline{j}$ does not destroy the distance $d \geq 4$ property, so the set of 16 vectors forms an $(8,16,4)$ code, $\overline{C}$.

According to the generalized block intersection numbers for this design relative to a block L of the design (cf. (4.7.9)), each block is complemented, so, for each $\underline{x} \in \overline{C}$, $\underline{x}+\underline{j}$ is also in $\overline{C}$. Furthermore, since blocks of T meet one another in exactly 2 or 0 places by (4.7.9) and since each of $\underline{0}$ and $\underline{j}$ meet all other vectors in $\overline{C}$ at distances 4, or 8, we see that two distinct code vectors of $\overline{C}$ are either at distance 4 from one another or are complementary. If two vectors are complementary, their sum is $\underline{j} \in \overline{C}$. If two vectors $\underline{x}$ and $\underline{y}$ are not complementary, they meet on two places. Since $b_2 = 3$ for a $S(3,4,8)$ design, there is a third vector $\underline{z}$ sharing with $\underline{x}$ and $\underline{y}$ those two places. But since $d \geq 4$, the remaining places of $\underline{x}$, $\underline{y}$, and $\underline{z}$ take care of the 6 other coordinate places of $V(8,2)$. As such $\underline{x}+\underline{y} = \underline{z}+\underline{j}$ which, in turn, is in $\overline{C}$. Therefore, $\overline{C}$ is linear. //

(7.2) Lemma: A linear $(8,16,4)$ code $\overline{C}$ is unique up to

a permutation of the 8 coordinate places of $V(8,2)$.

Proof: Choose a basis $\mathcal{B}$ for the linear subspace $\overline{C}$ of $V(8,2)$ so that the all-one vector is among those basis vectors, $\mathcal{B} = \{\underline{j}, \underline{x}_1, \underline{x}_2, \underline{x}_3\}$. Let G be an 8×4 zero-one matrix whose columns are the vectors of $\mathcal{B}$, i.e. G is a generator matrix of $\overline{C}$. The linear independence condition on basis vectors forces $\underline{x}_1$, $\underline{x}_2$, and $\underline{x}_3$ to be of weight 4 and to meet one another on precisely two places, i.e. $|\underline{x}_i \cdot \underline{x}_j| = 2$ for $i,j = 1,2,3$. But $|\underline{x}_1 \cdot \underline{x}_2 \cdot \underline{x}_3| = 1$, because if $\underline{x}_1$, $\underline{x}_2$, and $\underline{x}_3$ (i.e. $|\underline{x}_1 \cdot \underline{x}_2 \cdot \underline{x}_3| = 2$) meet on two places, $\underline{x}_3 + \underline{j} = \underline{x}_1 + \underline{x}_2$ and if they meet mutually on no places then $\underline{x}_3 = \underline{x}_1 + \underline{x}_2$ contradicting linear independence. Now three permutations can be found in S_8, φ_1, φ_2, φ_3 so that φ_1 permutes $\underline{x}_1$ to $(\underline{x}_1\varphi_1)^T = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1)^T$, so that φ_2 stabilizes $\underline{x}_1\varphi_1$ and permutes $\underline{x}_2\varphi_1$ to $x_2\varphi_1\varphi_2$ so that $(\underline{x}_2\varphi_1\varphi_2)^T = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)^T$, and so that φ_3 stabilizes both $\underline{x}_1\varphi_1$ and $\underline{x}_2\varphi_1\varphi_2$ and moves $\underline{x}_3\varphi_1\varphi_2$ to $\underline{x}_3\varphi_1\varphi_2\varphi_3$ with $(\underline{x}_3\varphi_1\varphi_2\varphi_3)^T = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)^T$. Thus G^T always can be put in the form

(7.3)
$$G^T = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} .$$

This shows that $\overline{C}$ is unique up to a motion of S_8. //

(7.4) Lemma: $S(3,4,8)$ is the design of the dependent 4-set in $V(3,2)$.

Remark: This lemma is quickly proved in either of two ways:

Proof 1: Given $V(3,2)$, each triple of vectors completes

uniquely to a dependent 4-set, so the dependent 4-sets form an $S(3,4,8)$, which by Lemmas (7.1) and (7.2) must be unique.

Proof 2: Given a design $S(3,4,8)$ and its spanning code $\overline{C}$, one can see via the $b_{i,j}^{L}$ for a block L of the design $S(3,4,8)$ (cf. (4.7.9)) that all blocks meet in an even number of places. Therefore in $\overline{C}$, all vectors are orthogonal to all other vectors from $\overline{C}$. In this way code vectors of $\overline{C}$ are the characteristic vectors of dependent sets in the $V(3,2)$ which vectors are rows of G (columns of G^T) as in (7.3). //

(7.5) Theorem: S_8 operates transitively on the set of 30 copies of $S(3,4,8)$ in $V(8,2)$.

Proof: We see via Lemma (7.2) that a design $S(3,4,8)$ is given by the set of weight 4 vectors in the linear span of the matrix G of (7.3). We shall count the number of distinct but isomorphic copies of $S(3,4,8)$ in $V(8,2)$ under the action of S_8 by counting the number of ways of obtaining the generator matrix G. From the complete design of all 4-tuples from the set of 8 coordinates of $V(8,2)$ we must choose vectors $\underline{x}_1$, $\underline{x}_2$, and $\underline{x}_3$ which will together with $\underline{j}$ form a generator matrix isomorphic to G. There are 70 ways that $\underline{x}_1$ can be chosen. The number of vectors $\underline{x}_2$ is then the number of 4-tuples from 8 that meet the 4-tuple corresponding to $\underline{x}_1$ in exactly two places. This number is $\binom{4}{2} \cdot \binom{8-4}{4-2} = 36$. Then the number of vectors $\underline{x}_3$ that can be chosen to meet $\underline{x}_1 \cdot \underline{x}_2, \underline{x}_1 \cdot (\underline{j}+\underline{x}_2), \underline{x}_2 \cdot (\underline{j}+\underline{x}_1)$,

and $\underline{j}+\underline{x}_1+\underline{x}_2+\underline{x}_1\underline{x}_2$, (i.e. the four disjoint pairs determined by $\underline{x}_1$ and $\underline{x}_2$) in one place each is $2^4 = 16$. Hence there are 70.36.16 matrices G.

Next we count the number of matrices G that correspond to a particular S(3,4,8) design, T. From T, the $\underline{x}_1$ may be chosen in $b_0 = 14$ ways, for the second, since $\underline{j}$, $\underline{x}_1$ and $\underline{x}_2$ must be linearly independent, $\underline{x}_2$ may not be the vector $\underline{j}+\underline{x}_1$ of T. Therefore, $\underline{x}_2$ may be chosen in 12 ways. Similarly due to the linear independence of $\mathcal{B} = \{\underline{j},\underline{x}_1,\underline{x}_2,\underline{x}_3\}$, $\underline{x}_3$ may be chosen from T in 14-6 = 8 ways as the vectors $\underline{x}_1,\underline{x}_2,\underline{x}_1+\underline{x}_2$, and their complements may not be chosen.

Therefore, there are 70.36.16/14.12.8 = 30 distinct copies of S(3,4,8) under the transitive action of S_8 on these 30 copies. //

(7.6) Corollary: The design S(3,4,8) has an automorphism group of order 8.7.6.4.

Proof: There are 14.12.8 = 8.7.6.4 motions under S_8 which stabilize a given S(3,4,8). //

(7.7) Theorem: A_8 acts $\frac{1}{2}$-transitively on the 30 copies of S(3,4,8) in V(8,2), yielding two orbits of 15 copies each.

Proof: Consider (as in the last Theorem (7.5)) the generator matrix G (7.3) of a S(3,4,8) design T. Given the two vectors $\underline{x}_1$ and $\underline{x}_2$ of G, there are 16 ways of choosing the vector $\underline{x}_3$ as we saw in the proof of Theorem (7.5).

But considering the design T, the 4 vectors $\underline{x}_3, \underline{x}_1 + \underline{x}_3, \underline{x}_2 + \underline{x}_3, \underline{x}_1 + \underline{x}_2 + \underline{x}_3$, and their complements all meet the two vectors $\underline{x}_1$ and $\underline{x}_2$ in such a way that each of these 8 vectors shares just one 1 with each of the pairs $\underline{x}_1 \cdot \underline{x}_2, \underline{x}_1 \cdot (\underline{j} + \underline{x}_2)$, $\underline{x}_2 \cdot (\underline{j} + \underline{x}_1)$, and $\underline{j} + \underline{x}_1 + \underline{x}_2 + \underline{x}_1\underline{x}_2$. Therefore, the set $\{\underline{j}, \underline{x}_1, \underline{x}_2\}$ can be complemented in 16 ways to generate $16/8 = 2$ distinct copies of $S(3,4,8)$.

Consider now the set of automorphisms $\varphi \in A_8$ which stabilizes $\underline{x}_1$ and $\underline{x}_2$. There are $2^4 = 16$ motions in S_8 stabilizing $\{\underline{x}_1, \underline{x}_2\}$ and therefore the 8 motions of A_8 which stabilize $\{\underline{x}_1, \underline{x}_2\}$ must yield 8 ways to complete $\{\underline{j}, \underline{x}_1, \underline{x}_2\}$ to generate $8/8 = 1$ unique $S(3,4,8)$. In other words, under $A_8, \underline{x}_1$ and $\underline{x}_2$ determine a unique copy of $S(3,4,8)$.

Considering just $\underline{x}_1$, this vector set $\{\underline{j}, \underline{x}_1\}$ completes to $\{\underline{j}, \underline{x}_1, \underline{x}_2, \underline{x}_3\}$ in 36.16 ways giving $36/12.16/8 = 6$ copies of $S(3,4,8)$ all sharing $\underline{x}_1$. But $\{\underline{j}, \underline{x}_1\}$ completes then to only $36/12.8/8 = 3$ copies of $S(3,4,8)$ under the action A_8.

Similarly under A_8, $\{\underline{j}\}$ may be completed to G in $70.36.8$ ways giving $70.36.8/14.12.8. = 15$ copies of $S(3.4.8)$ in an orbit under the action of A_8. //

(7.8) Corollary: Under the action of A_8 on the 30 copies of $S(3,4,8)$, all distinct copies T and S of $S(3,4,8)$ within one orbit share exactly one pair of

complementary vectors $\{\underline{x}_1, \underline{j} + \underline{x}_1\}$.

Proof: We see within the proof of Theorem (7.7) that the set $\{\underline{j}, \underline{x}_1\}$, completes to 3 copies of $S(3,4,8)$ under the action of A_8 all of which copies share only $\underline{x}_1$ and the complementary vector $\underline{j} + \underline{x}_1$. (Since if S and T were to share $\underline{x}_1$ and $\underline{x}_2 \neq \underline{j} + \underline{x}_1$, then $S = T$ due to the fact that $\{\underline{j}, \underline{x}_1, \underline{x}_2\}$ completes uniquely to a copy of $S(3,4,8)$ under the action of A_8.) //

(7.9) Corollary: Each pair of equivalence classes of 4-tuples from $V(8,2)$ and adjacent in G is contained in two copies of $S(3,4,8)$, one from each of the two orbits under action of A_8 .

Proof: Within the proof of Theorem (7.7) we saw that each pair of complementary 4-tuples was contained in two copies of $S(3,4,8)$. //

§8.8 Finding PG(3,2) within the Klein Quadric K

Thanks to the construction given in Section 8.7 we may now locate the points and lines of $PG(3,2)$ to be the 15 maximal cliques in G under the action of A_8 and the 35 points of K, Theorem (8.8). As an immediate byproduct of this approach we obtain a proof of the classical group isomorphism $A_8 \simeq PSL(4,2)$, Theorem (8.10).

Let K be the Klein quadric as defined in (3.8) and G be the graph as given in (5.1).

(8.1) Remark: A_8 acts $\frac{1}{2}$-transitively on the 30 maximal

cliques in G giving two orbits of 15 maximal cliques each, since the statement is merely a translation into terms relative to G of Theorem (6.4), Lemma (5.5), and Theorem (7.7).

(8.2) Let M be a fixed one of the orbits of 15 maximal cliques in G under the action of A_8 .

(8.3) Lemma: In M each point P of K (each vertex of G) is contained in precisely three maximal cliques of G . The $3.(7-1) = 18$ points other than P on these three maximal cliques are precisely all the vertices of G adjacent to P .

Proof: Interpreting Definition (3.9) and Corollary (7.8) into terms relative to G , one learns that each vertex of G (each complementary pair of weight 4 vectors in V(8,2)) is contained in precisely three maximal cliques of G (copies of S(3,4,8) in V(8,2)) under the action of A_8 . Furthermore, given a weight 4 vector $\underline{x}$ of V(8,2) corresponding to a vertex P of G , the number of vertices Q of G , which are adjacent to P is the number of ways of choosing representatives $\underline{y}$ of distinct equivalence classes of complementary vectors of V(8,2) with weight 4 which representatives meet $\underline{x}$ on two places, i.e. $|\underline{x} \cdot \underline{y}| = 2$. (This is seen from (3.9).) The number of vectors $\underline{y}$ meeting $\underline{x}$ on two places is $\binom{4}{2} \cdot \binom{4}{2} = 36$, but these fall into 18 classes of complementary pairs of weight 4 vectors, each representative of which meets $\underline{x}$ on two places. So P is adjacent in G to 18 vertices Q . Since the three maximal

cliques through P under A_8 are in one orbit, these maximal cliques share only P with one another due to Corollary (7.8). Hence contained in these cliques are 3.(7-1) = 18 other distinct vertices of G , each being adjacent to P . So all the vertices Q of G adjacent to P lie on these three maximal cliques. //

By Lemma (8.3) we may now define a design $\mathcal{D}$ as follows:

(8.4) Let points of $\mathcal{D}$ be the maximal cliques of M (defined in (8.2)). Let blocks of $\mathcal{D}$ be the sets of three maximal cliques of M which share mutually a single point. So a point of $\mathcal{D}$ is incident with a block of $\mathcal{D}$ if that maximal clique is contained in the set of three maximal cliques forming a block.

(8.5) Call blocks of $\mathcal{D}$ <u>lines</u>. Two lines of $\mathcal{D}$ <u>intersect</u> if they share a point of $\mathcal{D}$.

We have the correspondence of points of K (vertices of G) with lines of $\mathcal{D}$. We shall now proceed towards showing that points and lines of $\mathcal{D}$ are the points and lines of PG(3.2).

(8.6) <u>Lemma</u>: Vertices of G are adjacent iff the corresponding lines in $\mathcal{D}$ intersect.

<u>Proof</u>: Let P and Q be two adjacent vertices of G . By Lemma (8.3) there is just one maximal clique, π , of G through P and containing Q . So π is the maximal clique of M containing both P and Q . Hence, the lines

corresponding to P and Q in φ intersect. Conversely if two lines of φ intersect, the corresponding vertices P and Q of G lie on a maximal clique of M and are, by the definition of a clique, adjacent in G . //

(8.7) Theorem: The points and lines of φ form the points and lines of PG(3,2).

Proof: It is well known (c.f. Veblen and Young [37] and Dembowski [11]) that PG(3,2) is characterized by the following axiom system:

(i) Each two points determine a line.

(ii) Each two lines intersect in at most one point.

(iii) There are three points on each line.

(iv) (Pasch Axiom) Given any three non-collinear points and the three lines determined by these points, if another line meets any two of these lines then it meets also the third.

(v) There are 15 points.

From Lemma (8.3) follows (iii). Axiom (v) is by definition. Axiom (ii) follows from the fact that each adjacent pair P,Q of G is contained in precisely one maximal clique of G , due to Lemma (8.3).

In order to verify Axiom (i) we proceed as follows. A maximal clique π containes 7 points (Lemma (5.8)) and each of these points is contained in three maximal cliques of M , an orbit under A_8 , by Lemma (8.3). So counting, there are 2.(7) = 14 other maximal cliques in M meeting π

on a single point. Since A_8 is transitive on M, (i) follows.

Axiom (iv) follows from the existence of maximal cliques in G other than those from M. Let π_1, π_2, and π_3 be three non-collinear points of φ (i.e. three maximal cliques in M). Let ℓ_{12}, ℓ_{13}, and ℓ_{23} be the three lines of φ determined by those points and let P_{12}, P_{13}, and P_{23} be the corresponding vertices of G (these are distinct since the points π_1, π_2, and π_3 are not collinear). If ℓ is any other line of φ meeting two, say ℓ_{12} and ℓ_{13}, lines from $\{\ell_{12}, \ell_{13}, \ell_{23}\}$, then the corresponding point P of G is by Lemma (8.7) adjacent to both P_{12} and P_{13}. But vertices P_{12} and P_{13} are in a unique clique of M due to Lemma (8.3), so that $P, P_{12}P_{13}$ and P_{23} are all adjacent. Then again by Lemma (8.7), lines ℓ and ℓ_{23} meet. //

(8.8) Corollary: The 15 maximal cliques of G other than those of M correspond to the 15 planes of φ = PG(3,2).

Proof: By axioms (iv) and (v) 15 planes of φ exist. Each of these is then a set of 7 lines of φ mutually intersecting. By Lemma (8.7) these 7 lines correspond to a clique of G, but not to a clique of M. //

(8.9) Corollary: Three vertices of G which are mutually adjacent are collinear in PG(5,2) iff they correspond to planar fans of lines in PG(3,2), i.e. three lines that are concurrent and coplanar.

Proof: By Lemma (7.9) two adjacent vertices of G are contained in two maximal cliques, one from each orbit under A_8. Three adjacent vertices which are also collinear are therefore contained in two maximal cliques one corresponding to a point and the other to a plane of $PG(3,2)$. //

(8.10) Theorem: $A_8 \simeq \mathrm{Aut}(G) \simeq PSL(4,2)$.

Proof: $PSL(4,2)$ is by definition the group of collineations of $PG(3,2)$.

$A_8 \subseteq PSL(4,2)$: Let $\varphi \in A_8$, then φ induces an automorphism of G moving vertices while stabilizing each of the sets of points, of lines and of planes. Because of Corollary (8.9) and the fact that φ preserves linearity in $PG(5,2)$ and adjacency in G, $\bar{\varphi}$ preserves linearity in $PG(3,2)$.

Conversely:

$PSL(4,2) \subseteq A_8$: Let $\bar{\varphi} \in PSL(4,2)$, then φ induces a motion φ^* of G stabilizing each of the orbits of maximal cliques in G under A_8. $\varphi^* \in \mathrm{Aut}(G)$ by virtue of Lemma (8.7). But φ^* extends uniquely to a motion φ of $PG(5,2)$ and $V(8,2)$ via Corollary (6.5). Finally $\varphi \in \bar{O}_6(+,2) \simeq A_8$ due to Corollary (8.9). //

(8.11) Corollary: $S_8 \simeq$ the group of all collineations and correlations of $PG(3,2) = P\Gamma L(4,2)$.

Proof: The design $\mathcal{D}$ of Definition (8.4) is isomorphic to $PG(3,2)$ no matter which orbit of 15 maximal cliques of G under A_8 is used. With one of these orbits chosen to

represent points, a motion of $S_8 \setminus A_8$ induces a motion of PG(3,2) preserving linearity but exchanging the roles of points and planes. This motion is a collineation of the PG(3,2) defined relative to the former orbit. Hence, $S_8 \subseteq P\Gamma L(4,2)$. The converse inclusion is similarly shown. //

§8.9 Eight Objects in PG(5,2) Permuted by PSL(4,2) $\simeq A_8$

Now that we have $PSL(4,2) \simeq A_8$ (Theorem 8.10), we can recall the definition of the graph H (5.2) and the Lemma (5.8) stating that there are eight simplices of PG(5,2) disjoint from the Klein quadric K (3.8), which eight simplices not only have their 7 vertices located off K, but also (by Definition (5.4)) their $\binom{7}{2} = 21$ third points on the $\binom{7}{2} = 21$ lines joining pairs of vertices of such a simplex located off K. There are only 8 simplices of PG(5,2) of this nature, since any such simplex must be a maximal clique of H of 7 vertices. These are 8 geometrical objects in PG(5,2) permuted by PSL(4,2):

(9.1) Theorem: PSL(4,2) faithfully permutes the 8 simplices whose 7 vertices and whose $\binom{7}{2} = 21$ third points on the 1-skeleton, the set of lines joining these 7 vertices, are totally off K.

Proof: Since by Lemma (5.6) the 8 maximal cliques of graph H from (5.2)) are coordinatized under V(8,2) by 7 pairs of coordinates from V(8,2) which all share one coordinate, these 8 maximal cliques correspond one to one to the coordinates of V(8,2). Furthermore, these correspond

to 8 simplices of PG(5,2) whose 8 vertices and 21 third points on the 1-skeleton of such a simplex are off K (Lemma (5.8)). Then Theorem (8.10) shows that PSL(4,2) permutes these. The action is faithful because if all 8 simplices are fixed, all the 8 coordinates of V(8,2) must be fixed and the motion must be the identity. //

§8.10 Line Coordinates for PG(3,2) and 8 Objects in PG(3,2) Permuted by PSL(4,2)

It has finally been established that lines of PG(3,2) are permuted by PSL(4,2) exactly as the complementary pairs of weight 4 vectors of V(8,2) are permuted by A_8, and so that lines of PG(3,2) intersect iff representative weight 4 vectors share ones in exactly two coordinate places.

(10.1) Theorem: There is a one to one correspondence φ from the 35 lines to the 35 sets of complementary 4-tuples from a given set of 8 letters so that PSL(4,2), operating on the 35 lines, is mapped isomorphically to A_8, operating on the 8 letters.

Proof: Let the set X of 8 letters correspond to 8 standard basis coordinate vectors of a V(8,2). Then Theorem (6.4) shows that corresponding to Definitions (2.6) of $PG(5,2) \subset V(8,2)$, (3.8) of the Klein quadric K in PG(5,2), and (5.1) of the graph G in K, $A_8 \simeq \mathrm{Aut}(G)$. Furthermore, defining $\mathcal{P}$ as in (8.4), we have by Theorem (8.7) that $\mathcal{P}$ is isomorphic as a geometry to PG(5,2) and that $PSL(4,2) \simeq \mathrm{Aut}(G) \simeq A_8$ by Theorem (8.10). This gives a

correspondence φ between lines of PG(3,2) and complementary pairs of 4-tuples from the set X of 8 letters via Theorem (8.7), Lemma (8.6), and Definitions (5.2), (3.9), and (2.6), so that lines of PG(3,2) intersect iff representative 4-tuples from X share precisely two letters. It follows that $PSL(4,2) \simeq A_8$ under φ . //

(10.2) Throughout this section let $\overline{X}$ be the set of 8 letters $X := \{a,b,c,d,e,f,g,h\}$ on which A_8 acts isomorphically to PSL(4,2) according to Theorem (10.1).

Since Theorem (10.1) gives 8 letter coordinates for lines of PG(3,2), sets of lines can also be coordinatized by these 8 letters. Since points and planes of PG(3,2) are each characterized by special sets of lines, we have:

(10.3) Lemma: The 15 points and the 15 planes of PG(3,2) are each coordinatized by the 30 copies of S(3,4,8) in the V(8,2) whose 8 standard basis vectors are the 8 elements of X .

Proof: Points of PG(3,2) are characterized by the 7 lines of PG(3,2) through the point. Planes are characterized by the 7 lines on that plane. Each set of 7 lines forms a maximal clique of 7 mutually intersecting lines in PG(3,2) and then the pairs of complementary 4-tuples coordinatizing those 7 lines form a copy of S(3,4,8). Then by Lemma (5.5), Definition (8.4), Theorem (8.7), and Corollary (8.8) the result follows. //

Now we shall proceed to establish just what sets

of lines of $PG(3,2)$ correspond in a one to one fashion to the 8 letters on which A_8 acts.

(10.4) Define a spread in $PG(3,2)$ to be a set of lines which are mutually disjoint and so that every point of $PG(3,2)$ is contained in exactly one of these lines. It is clear that there are $15/3 = 5$ lines in each spread of $PG(3,2)$. This definition corresponds to D. M. Mesner's use of the word in [26].

(10.5) Lemma: Triples from the set X of 8 letters on which A_8 acts isomorphically to $PSL(4,2)$ correspond under this isomorphism to the $\binom{8}{3} = 56$ spreads of $PG(3,2)$. The five lines in a spread all have representative 4-tuples which contains the triple corresponding to that spread.

Proof: Given any triple, say $\{a,b,c\} \subset X$, there are precisely 5 lines of $PG(3,2)$ whose corresponding equivalence classes of complementary 4-tuples from X have a representative containing $\{a,b,c\}$. Since by Theorem (10.1) lines in $PG(3,2)$ intersect iff their representative 4-tuples share precisely two letters, the 5 lines corresponding to $\{a,b,c\}$ are mutually disjoint. Together the 5 lines contain all $3.5 = 15$ points of $PG(3,2)$, so they form a spread of $PG(3,2)$ by Definition (10.4).

To show that the $\binom{8}{3} = 56$ spreads obtained in this way are all the spreads of $PG(3,2)$ we note that representative 4-tuples for three mutually disjoint lines having their representatives share three letters can be chosen in the following two ways:

of lines of $PG(3,2)$ correspond in a one to one fashion to the 8 letters on which A_8 acts.

(10.4) Define a spread in $PG(3,2)$ to be a set of lines which are mutually disjoint and so that every point of $PG(3,2)$ is contained in exactly one of these lines. It is clear that there are $15/3 = 5$ lines in each spread of $PG(3,2)$. This definition corresponds to D. M. Mesner's use of the word in [26].

(10.5) Lemma: Triples from the set X of 8 letters on which A_8 acts isomorphically to $PSL(4,2)$ correspond under this isomorphism to the $\binom{8}{3} = 56$ spreads of $PG(3,2)$. The five lines in a spread all have representative 4-tuples which contains the triple corresponding to that spread.

Proof: Given any triple, say $\{a,b,c\} \subset X$, there are precisely 5 lines of $PG(3,2)$ whose corresponding equivalence classes of complementary 4-tuples from X have a representative containing $\{a,b,c\}$. Since by Theorem (10.1) lines in $PG(3,2)$ intersect iff their representative 4-tuples share precisely two letters, the 5 lines corresponding to $\{a,b,c\}$ are mutually disjoint. Together the 5 lines contain all $3.5 = 15$ points of $PG(3,2)$, so they form a spread of $PG(3,2)$ by Definition (10.4).

To show that the $\binom{8}{3} = 56$ spreads obtained in this way are all the spreads of $PG(3,2)$ we note that representative 4-tuples for three mutually disjoint lines having their representatives share three letters can be chosen in the following two ways:

{a,b,c,d }
{a,b,c, e }
{a,b,c f}

or

{a,b,c,d }
{a,b,c, e }
{a,b, d,e } .

Each of these completes uniquely to a set of 5 representative 4-tuples for a spread, the first of which has all representatives containing {a,b,c} and the second of which has the complements of all representatives containing {f,g,h} . Therefore each spread corresponds to one unique triple from X . //

(10.6) Lemma: Two spreads of PG(3,2) share 0, 1, or 2 lines of PG(3,2) according as the triples from X corresponding to those two spreads share 1, 2, or 0 letters respectively.

Proof: The two spreads {a,b,c}, {a,b,d} share only the line {{a,b,c,d} , {e,f,g,h}} . The two spreads {a,b,c} , {d,e,f} both share only the two lines given by {{a,b,c,g} , {d,e,f,h}} and {{a,b,c,h}, {d,e,f,g}} . None of the 5 lines of {a,b,c} are among those of the spread {a,d,e} , so two spreads sharing one letter are disjoint spreads. //

(10.7) Definition: The lines in a set of 6 spreads of PG(3,2) which pairwise share one line of PG(3,2) is

called a linear complex of lines of PG(3,2) . This definition is equivalent in the setting of PG(3,2) to the definition of linear complex given by Todd in [35], but this equivalence shall not be established as we shall only use the definition as a convenient name.

(10.8) Lemma: The $\binom{8}{2} = 28$ pairs of letters of X correspond to the 28 linear complexes in PG(3,2) .

Proof: There are two types of sets of four spreads of PG(3,2) which pairwise share one line of PG(3,2) . Using Lemma (10.6) these are:

$$\begin{array}{l} \{a,b,c\ \ \ \ \ \ \} \\ \{a,b,\ \ d\ \ \ \} \\ \{a,b,\ \ \ \ e\ \} \\ \{a,b,\ \ \ \ \ \ f\} \end{array} \qquad \text{and} \qquad \begin{array}{l} \{a,b,c\ \ \} \\ \{a,b,\ \ d\} \\ \{a,\ \ c,d\} \\ \{\ \ b,c,d\} \ . \end{array}$$

The second of these cannot be completed to a set of even 5 spreads which pairwise share one line, whereas the first can be completed to the linear complex:

$$\begin{array}{l} \{a,b,c\ \ \ \ \ \ \ \ \} \\ \{a,b,\ \ d\ \ \ \ \ \ \} \\ \{a,b,\ \ \ \ e\ \ \ \ \} \\ \{a,b,\ \ \ \ \ \ f\ \ \ \} \\ \{a,b,\ \ \ \ \ \ \ g\ \ \} \\ \{a,b,\ \ \ \ \ \ \ \ \ h\} \ . \end{array}$$

Therefore, linear complexes correspond one to one to pairs of the 8 letters of X . //

(10.9)

l spre

letter

Proof

pair

(10.1(

is a

spread

[10],

(10.1

PG(3,

Proof

pairs

a fix

to on

lette

(10.1

of li

so th

(10.9) Lemma: Two linear complexes of PG(3,2) share 0 or 1 spread of PG(3,2) iff their corresponding pairs of letters from X share 0 or 1 letters respectively.
Proof: {a,b} and {a,c} share the spread {a,b,c} . The pair {a,b} and {c,d} share no spread. //
(10.10) Definition: A heptad of linear complexes in PG(3,2) is a set of 7 linear complexes which pairwise share one spread. This name is used by Conwell, Edge, and Jonsson in [10], [14], and [19], respectively.
(10.11) Lemma: The eight heptads of linear complexes in PG(3,2) correspond to the eight letters of X themselves.
Proof: Using (10.9) and (10.10), a set of more than three pairs of X which mutually share one letter must all contain a fixed one of the letters of X . So each heptad corresponds to one of the letters of X . //

Lemma (10.11) plus the fact that A_8 permutes the 8 letters of X faithfully proves:
(10.12) Theorem: There are 8 heptads of linear complexes of lines in PG(3,2) which A_8 permutes faithfully in a way so that $A_8 \simeq PSL(4,2)$.

CHAPTER 9

The Uniqueness of the XNR-Design Within the Geometry of V(4,2)

§9.1 Introduction

It is the purpose of this chapter to complete the proof of the uniqueness of the XNR-design, Theorem (9.5.1), by showing that the design can be constructed within the context of $V(4,2)$ in only one way (up to an automorphism of $V(4,2)$). Chapter 7 has shown that the weight 6 code words in any XNR code (containing $\underline{O}$) are embeddable in $V(4,2)$, Theorem (7.5.1) and Lemma (7.5.11). From the fact that the weight 6 code words form an XNR-design, Definition (4.7.3) and Remark (4.3.4), it follows that any XNR-design can be embedded in $V(4,2)$. Therefore, in order to prove that the XNR-design is unique, it suffices to show that it can be constructed within $V(4,2)$ in only one way (up to automorphism).

Within the context of $V(4,2)$, the uniqueness proof proceeds as follows. First, in Section 9.2, necessary conditions for the existence of the XNR-design, D, are noted. The 112 blocks of D sub-divide into sets of 42 and 70 blocks according as the blocks contain the point corresponding to $\underline{O} \in V(4,2)$ or not. These 42 and 70 blocks

form designs S and L respectively on the point set $PG(3,2) = V(3,2) - \{\underline{0}\}$. Moreover these blocks indicate simplices and skew line pairs, respectively, in $PG(3,2)$. Design L gives rise to a one to one correspondence, s , between all the lines of $PG(3,2)$ and some of the spreads of $PG(3,2)$. Then, in Sections 9.3 and 9.4, it is shown that, up to an automorphism of $PG(3,2)$, correspondence s and designs L and S are unique. Finally, in Section 9.5, it is shown that the XNR-design D is unique up to an automorphism of $V(4,2)$. Designs S and L and correspondence s , which are referred to throughout this chapter, are defined in Section 9.2.

As a corollary of the uniqueness of the XNR-design, D , we obtain the fact that D is coincident with the design constructed in Chapter 5, Theorem (5.3.9). This leads to the fact that the automorphism group of the XNR-design is $A_7 + T(4)$, i.e. A_7 extended by the groups of translations of $V(4,2)$, Theorem (5.2) .

§9.2 Necessary Conditions for the Existence of an XNR-Design: Designs S and L and Correspondence s

Given an XNR-design D , from Theorem (7.5.11) all of the 112 blocks, when viewed as weight 6 vectors in $V(16,2)$ are characteristic functions of dependent 6-sets of vectors of $V(4,2)$. Since dependent sets in $V(4,2)$ are given relative to $\underline{0} \in V(4,2)$ and since $b_1 = 42$ for design D (c.f. (6.4.b)), there are 42 weight 6 vectors of D

containing the coordinate corresponding to $\underline{0}$ and 70 not containing $\underline{0}$. Interpreted in terms of characteristic functions relative to $PG(3,2) = V(4,2) \setminus \{\underline{0}\}$, we have:

(2.1) Lemma: When the point set is restricted to $PG(3,2) = V(4,2) \setminus \{\underline{0}\}$, the 112 blocks of the design D subdivide into a set of 42 weight 5 blocks and a set of 70 weight 6 blocks. Their respective weight 5 and 6 vectors are characteristic functions of simplices and pairs of skew lines in $PG(3,2)$.

Proof: Let $\underline{e}_1$ be the basis vector of $V(16,2)$ corresponding to $\underline{0} \in V(4,2)$. By $b_1 = 42$ for D , the 42 weight 6 vectors containing a 1 in the coordinate $\underline{e}_1$ place locate a dependent set of 5 points in $PG(3,2)$. Since no two points in any $PG(n,2)$ are dependent, this set must have no three points dependent (collinear) and no four dependent (coplanar). As such each dependent set of five points is a simplex in $PG(3,2)$. For the 70 weight 6 vectors containing a 0 in the coordinate corresponding to $\underline{e}_1$, each yields a set of 6 dependent points of $PG(3,2)$. Simplices have in $PG(3,2)$ at most 5 points so at least 3 of the 6 points must be dependent (collinear), but then the complementary set must be also dependent of cardinality at least 3. So such a dependent 6-set is necessarily a pair of skew lines in $PG(3,2)$. //

(2.2) Corollary: The 42 simplices and 70 pairs of skew lines from $PG(3,2)$ form, respectively, a $4-(2,5,15)$ design S and a $10-(2,6,15)$ design L , each with $d \geq 6$.

Proof: According to (4.15), the 42 blocks of D having a 1 in the place, $\underline{e}_1$, form the derived design of D which is a 4-(3-1,6-1,16-1) design, S . The other 70 blocks then form a (14-4)-(3-1,6-0,16-1) design L , because D is by (4.1.4) also a 14-(2,6,16) design. These designs clearly inherit $d \geq 6$ being no more than a subset of vectors already with the $d \geq 6$ property. Hence these sets of 42 simplices and 70 pairs of skew lines must be 4-(2,5,15) and 10-(2.6.15) designs with $d \geq 6$. //

(2.3) So if D is any XNR-design embedded in V(4,2) , its 112 blocks define on the point set PG(3,2) a design $\underline{S}$ of 42 simplices of PG(3,2) and a design $\underline{L}$ of 70 skew line pairs of PG(3,2) . Designs S and L are 4-(2,5,15) and 10-(2,6,15) designs with $d \geq 6$, respectively, by Corollary (2.2).

Since D is a 3-design, each triple of points from PG(3,2) occurs a total of $b_3 = 4$ times among the blocks of the designs S and L . Since triples of points of PG(3,2) are of two types, collinear or non-collinear,

(2.4) we shall call these sets lines and triangles of PG(3,2) , respectively.

(2.5) Lemma: Each triangle of PG(3,2) is contained in exactly one of the blocks of S .

Proof: Since Corollary (2.2) shows that S has $d \geq 6$, two simplices of the design cannot share a triangle. Hence, each triangle must be contained in a unique simplex. There

are $\binom{15}{3}$ triples in PG(3,2) and of these, $15.14.1/3! = 35$ triples are lines, so there are $\binom{15}{3} - 35 = 420$ triangles of PG(3,2) . But there are then $42.\binom{5}{3} = 420$ triangles each contained uniquely in the 42 blocks of the simplex design, S . Therefore, each triangle of PG(3,2) is in exactly one block. //

(2.6) Corollary: Each triangle of PG(3,2) is contained in exactly three blocks of L .

Proof: Each triple of D is in precisely 4 blocks, and each triangle is in a unique simplex, by (2.5). //

(2.7) Lemma: Each line of PG(3,2) is contained in exactly four blocks of L . Each such line and the four others skew to it from each of the four blocks form a spread in PG(3,2) .

Proof: Since no triple in a simplex can be dependent (collinear), each line of PG(3,2) must be in 4 blocks of L . Consider the 4 blocks from L containing a fixed line ℓ_1 of PG(3,2) . Let ℓ_2 , ℓ_3 , ℓ_4 , and ℓ_5 be the other lines skew to ℓ_1 so that $\{\ell_1, \ell_i\}$ i = 2,3,4,5 are those four blocks of L . Because $d \geq 6$ in L (Corollary (2.2)), the pairs $\{\ell_i, \ell_j\}$, i,j = 2,3,4,5, $j \neq i$, must also be skew. Therefore $\{\ell_i \mid i = 1,2,3,4,5\}$ is a spread of PG(3,2) (cf. Definition (8.10.5)). //

(2.8) Theorem: Corresponding to each design L in PG(3,2) there is an injection, s , of the lines of PG(3,2) into the spreads of PG(3,2) such that each of the four blocks of L containing a line ℓ contains also a second line

from the spread $s(\ell)$.

Proof: By Lemma (2.7) the four blocks of L containing a given line ℓ_1 of PG(3,2) determine a well-defined spread, $s(\ell_1) = \{\ell_1, \ell_2, \ell_3, \ell_4, \ell_5\}$ in PG(3,2), so that $\{\ell_1, \ell_i\}$ for $i = 2,3,4,5$, are blocks of L . Should any two lines, say ℓ_1 and ℓ , from PG(3,2) determine the same spread, then $s(\ell_1) = s(\ell)$ so that $\ell \in s(\ell_1)$. Let ℓ be ℓ_2 w.l.o.g. Now Lemma (2.7) applied to $s(\ell_2)$ implies that $\{\ell_2, \ell_i\}$ for $i = 3,4,5$ are also blocks of L . Hence these are blocks of D . Then $\{\ell_1, \ell_4\}$ and $\{\ell_2, \ell_3\}$ are two disjoint blocks of D . But since $b^B_{0,6} = 0$ for the generalized block intersection numbers for D relative to a block B of this design D (cf. (6.4.6)), D has no block disjoint from any given block B of D . This contradiction forces the spreads $s(\ell_1)$ and $s(\ell_2)$ to be distinct. Thus the correspondence s is one to one. //

(2.9) Define s to be any of the one to one correspondences determined by a design L in PG(3,2) .

§9.3 The Uniqueness Under A_8 of the Correspondence s and Design L

(3.1) Lemma: The stabilizer of a line in PG(3,2) is transitive on the set of 8 spreads of PG(3,2) which contains that line.

Proof: Since there is always an even permutation of X mapping any 4-tuple from X to any other, A_8 is transitive on lines of PG(3,2). So w.l.o.g. we may consider a line

ℓ of PG(3,2) to be coordinatized by $\{\{a,b,c,d\},\{e,f,g,h\}\}$. By Lemma (8.10.6) this line is contained in the 8 spreads: $\{a,b,c\}$, $\{a,b,d\}$, $\{a,c,d\}$, $\{b,c,d\}$, $\{e,f,g\}$, $\{e,f,h\}$, $\{e,g,h\}$, and $\{f,g,h\}$. Since these 8 triples are completely contained in either of the 4-tuples corresponding to the line ℓ, there is a motion $\varphi \in A_8$ which stabilizes ℓ and moves any of these triples to any other of these triples. //

(3.2) Theorem: Any one to one correspondence s of lines of PG(3,2) to 35 of the spreads of PG(3,2) such that each line ℓ' of PG(3,2) together with the four other lines of the spread $s(\ell')$ form a block of L, is uniquely determined by any one line and its corresponding spread.

Proof: First consider any two skew lines. They must have 8 letter coordinates which by Theorem (8.10.1) have representatives sharing 1 or 3 letters. There is a motion φ of A_8 sending the coordinates of a line ℓ_1 to $\{\{a,b,c,d\}, \{e,f,g,h\}\}$. Then a further motion φ_2 of A_8 may be chosen to send the coordinates of a line ℓ_2 which is skew to ℓ_1 to $\{\{a,e,f,g\}, \{b,c,d,h\}\}$. ($A_8$ is shown to be transitive on pairs of skew lines in this way.) Now it is clear that ℓ_1 and ℓ_2 are both in the two spreads $\{b,c,d\}$ and $\{e,f,g\}$, (cf. (8.10.6)).

Now let $s(\ell_1) = \{b,c,d\}$. If s is to generate the blocks of a 10-(2,6,15) design L, with $d \geq 6$, as indicated in the hypotheses of this lemma, then $\{\ell_1, \ell_2\}$ must be a block of L. Now ℓ_2 must correspond to one of the two spreads containing $\{\ell_1, \ell_2\}$ since this set is

already a block of L. But ℓ_2 does not correspond to $\{b,c,d\} = s(\ell_1)$ by Theorem (2.8), and hence, necessarily $s(\ell_1)$ in the spread $\{b,c,d\}$ must correspond by s to the spread $\{y,z,w\}$ for $\{y,z,w\} \subset \{e,f,g,h\}$. Note that each of the five lines with correspondence s defined already, correspond to the spread given by that triple which together with the letter a form a 4-tuple representative for the line.

Now by considering the $4.(5-2) = 12$ other lines in the four spreads $\{y,z,w\} \subset \{e,f,g,h\}$ corresponding under s to the other four lines in the initial spread $\{b,c,d\}$, one sees that each of these lines must correspond under s to that triple which together with the letter a forms a 4-tuple representative of the line. For example, consider the spread $\{e,f,g\}$ and its five lines:

$$\{\{a,b,c,d\}, \{e,f,g,h\}\} = \ell_1$$
$$\{\{b,c,d,h\}, \{e,f,g,a\}\} = \ell_2$$
$$\{\{a,c,d,h\}, \{e,f,g,b\}\} = \ell_3$$
$$\{\{a,b,d,h\}, \{e,f,g,c\}\}$$
$$\{\{a,b,c,h\}, \{e,f,g,d\}\} \quad .$$

Since $\{\ell_2, \ell_3\}$ is already necessarily a block of L, $s(\ell_3) = \{c,d,h\}$.

Finally, by considering each of the 18 other lines from $PG(3,2)$, one finds that there is exactly one spread that can correspond to each of these lines. This spread

is the one whose triple together with the letter a forms a 4-tuple representative of that line. //

(3.3) Corollary: If $s(\ell) = \{b,c,d\}$ for the line ℓ given by $\{\{a,b,c,d\}, \{e,f,g,h\}\}$, then $s(\ell') = \{x,y,z\}$ where $\{\{a,x,y,z\}, \{w,m,n,p\}\}$ is the 8 coordinate name for ℓ', and $\{x,y,z,w,m,n,p\} = X \setminus \{a\}$.

(3.4) Theorem: Up to a motion of $PG(3,2)$, the design L is unique.

Proof: By Theorem (2.8), there must be a correspondence s mapping the lines of $PG(3,2)$ to 35 of the spreads of $PG(3,2)$ so that the correspondence locates the blocks of the design L. Up to a permutation A_8 the initial choice of the spread $s(\ell)$ corresponding to ℓ is unique for any fixed line ℓ of $PG(3,2)$, by Lemma (3.1). Then Theorem (3.2) shows that s is completely determined by these initial conditions. //

(3.5) Theorem: The automorphism group of the design L is A_7.

Proof: By Lemma (2.7) each line of $PG(3,2)$ is contained in four blocks of L. Any motion φ of the points of L, i.e. the points of $PG(3,2)$, which sends also blocks to blocks must send the four blocks through one line to the four blocks through another line. Hence φ induces a collineation φ^* of $PG(3,2)$ so $\varphi^* \in PSL(4,2) \simeq A_8$. But φ^*, as a collineation of $PG(3,2)$, permutes the set of 56 spreads of $PG(3,2)$. By Corollary (3.3), φ^* must move these 56 spreads in two sets - the set of 35 spreads

corresponding under s to lines of $PG(3,2)$ whose triples are from $X \setminus \{a\}$, and the set of 28 other spreads whose triples contain the letter a. Since the subgroup of A_8 which fixes the letter a is A_7, $Aut(L) \subseteq A_7$.

If $\varphi \in A_7$ where A_7 operates on $X \setminus \{a\}$, then φ induces a unique mapping s agreeing with the hypotheses of Theorem (2.8) and the correspondence given in Corollary (3.3). Therefore, the equivalent $1O-(2,6,15)$ design $(L\varphi)$ with $d \geq 6$ induced by φ has exactly the same correspondence s and hence the same blocks. Therefore $A_7 \subseteq Aut(L)$. //

(3.6) Corollary: A_7 is 1-transitive on blocks of L.

Proof: Consider for each line of $PG(3,2)$ only the representative 4-tuple which contains the letter a. Then on $X \setminus \{a\}$, lines correspond to triples. Exactly these triples are also the spreads under the correspondence s, as in Corollary (3.3). This means that the two lines of a typical block of L have corresponding triples which are disjoint triples chosen from $X \setminus \{a\}$. Since A_7 is transitive on pairs of disjoint triples chosen from $X \setminus \{a\}$, A_7 is transitive on blocks L. //

§9.4 The Uniqueness of the Design Pair S,L

We know from Section 9.3 that design L and its related correspondence s are unique up to a motion of $PSL(4,2)$. Aiming towards the uniqueness of D we show in this section that there is a unique design S that can extend a fixed design L to D. We do not prove that design S is

unique, but rather the uniqueness of the pair S,L which can be extended to D.

(4.1) Theorem: Given $PG(3,2)$ and the (unique) design L, there is a unique design S which together with L can be extended to an XNR-design D.

Proof: Assume that S and L are respectively $4\text{-}(2,5,15)$ and $10\text{-}(2,6,15)$ designs which build an XNR-design D by attaching a sixteenth point to the point set of these two designs. Considering the 15 point set to be the set of points of $PG(3,2)$, O may be then augmented to each simplex and to none of the pairs of skew lines so that the resulting design D has $V(4,2)$ as its point set. Then by Lemma (2.5), it is necessary that each triangle from $PG(3,2)$ be located in one and only one simplex of S.

(4.2) Furthermore, since $d \geq 6$ in D, two blocks of D, one from S and one from L must overlap on at most three points of $PG(3,2)$.

Consider any one triangle of $PG(3,2)$. Label its three lines as ℓ_1, ℓ_2, ℓ_3. In $PG(3,2)$ this triangle completes to a Fano plane. Let the seventh point of this plane, which is not on any of the three lines ℓ_1, ℓ_2, or ℓ_3, be called P. Through P pass seven lines of $PG(3,2)$, three of which occur on this plane. Let the four lines through P and not contained in this plane be labeled m_1, m_2, m_3 and m_4. By the necessary correspondence s, as given in Theorem 2.8) and Definition (2.9) spreads $s(\ell_1), s(\ell_2)$, and $s(\ell_3)$ must correspond to lines ℓ_1, ℓ_2, ℓ_3 of the fixed

triangle so that ℓ_i together with each of the other four lines in the spread $s(\ell_i)$ must form a block of L, for $i = 1,2,3$. Since one line of any spread, by Definition (8.10.5), passes through each point of $PG(3,2)$, one of the four lines m_j, $j = 1,2,3,4$, together with each ℓ_i, $i = 1,2,3$, must form a block of L. But furthermore, since $d \geq 6$ in design L, and since any two of the lines ℓ_i for $i = 1,2,3$ meet on a point, each ℓ_i, $i = 1,2,3$ must form a block with a distinct one of the lines m_j, $j = 1,2,3,4$. So w.l.o.g. let $\{\ell_i, m_i\}$, $i = 1,2,3$ be blocks of L, i.e. let m_i be contained in the spread $s(\ell_i)$ for $i = 1,2,3$.

Now, any triangle of $PG(3,2)$ is contained in four simplices of $PG(3,2)$, namely the three points of the triangle P_{12}, P_{13}, P_{23} (for $P_{ij} = \ell_i \cap \ell_j$, $i, j = 1,2,3$, $i \neq j$), together with the two points of each of the four lines m_j, $j = 1,2,3,4$ other than P. If the simplex to be chosen through $\{P_{12}, P_{13}, P_{23}\}$ contains the two points of m_j for $j = 1,2,3$ other than P, say the two points Q_1 and R_1 of m_1, then the simplex $\{P_{12}, P_{13}, P_{23}, Q_1, R_1\}$ of S would meet the block $\{\ell_1, m_1\}$ of L in the four points of $\{P_{12}, P_{13}, Q_1, R_1\}$, contradicting the fact stated in (4.2) that a block of L and a block of M must share at most three points.

Therefore, through $\{P_{12}, P_{13}, P_{23}\}$ can be chosen only the simplex $\{P_{12}, P_{13}, P_{23}, Q_4, R_4\}$ where Q_4 and R_4 are the two points of m_4 other than P. Hence, the triangle can

be contained in at most one simplex that can be used for the design S .

Now the existence of the XNR-design D as guaranteed by Remark (4.3.4) (and by Theorem (5.3.9)) shows together with Lemma (2.5) that each triangle is contained in exactly one simplex of S . //

(4.3) Corollary: The design S of 42 simplices as referred to in Theorem (4.1) has $d \geq 6$.

Proof: The uniqueness of the system as guaranteed by Theorems (3.4) and (4.1) together with the existence of the systems shown in Theorem (5.3.9) yields the distance condition $d \geq 6$ for S as well for L and D . //

(4.4) Theorem: The automorphism group of S is A_7 .

Proof: By Theorem (3.5) the automorphism group of design L is A_7 . Each motion of A_7 then permutes the 15 points of $PG(3,2)$ and stabilizes the set of 70 pairs of skew lines of $PG(3,2)$ forming blocks of L . As such, since the 70 block design L implies the existence of 42 simplices uniquely chosen relative to L , each motion φ of $Aut(L) \simeq A_7$ moves points of $PG(3,2)$ and stabilizes the set of 42 simplices in S . Hence $A_7 \subseteq Aut(S)$.

Conversely, given any $\varphi \in Aut(S)$, consider the four blocks of S containing a given pair of points. As φ moves points of $PG(3,2)$ to points and simplices of S to simplices of S , φ must move a pair of points together with the four blocks of S containing that pair to another

pair of points together with its four blocks. Counting all the points in these four blocks with use of $d \geq 6$, four blocks containing that pair involve 14 of the 15 points of PG(3,2). By Lemma (2.7) this fifteenth point must be collinear with that pair. Hence, φ moves lines of PG(3,2) to lines and therefore is a collineation of PG(3,2). But as a collineation of PG(3,2), φ permutes spreads of PG(3,2). Were the 35 spreads corresponding to the design L, which according to the hypotheses of Theorem (4.1) exists simultaneously with S, not stabilized by φ, then φ would not stabilize the 70 blocks of L. Then the correspondence s would not stabilize the 42 blocks of S, and $\varphi \notin Aut(S)$, a contradiction.

Therefore φ induces an automorphism of L showing that $Aut(S) \subseteq A_7$.

As a result, $Aut(S) \simeq A_7 \simeq Aut(L)$. //

§9.5 The Uniqueness of the XNR-Design D

(5.1) Theorem: Up to a permutation of the 16 coordinates of V(16,2), the XNR-design D is unique.

Proof: As seen in Theorem (6.5.9), each XNR-design D generates a (16,256,6) code C, where standard basis vectors of V(16,2) are the points of D. Then by Theorem 7.5.11) the weight 6 vectors in C, i.e. those corresponding to blocks of D must be characteristic functions of dependent 6-sets in V(4,2). Then by letting

an arbitrary coordinate place of $V(16,2)$ correspond to $\underline{O} \in V(4,2)$, these dependent 6-sets in $V(4,2)$ yield a design L according to Lemma (2.1) and Corollary (2.2). Design L is unique, Theorem (3.4), up to a collineation of $PG(3,2)$ which is a permutation of the 15 coordinates of $V(16,2)$ other than the one corresponding to $\underline{O} \in V(4,2)$. Furthermore, design L induces a unique design S which together with L builds design D whose points are the 16 vectors of $V(4,2)$, by Theorem (4.1). Hence, even after arbitrarily fixing the coordinate place of $V(16,2)$ corresponding to $O \in V(4,2)$, there is a permutation of the other 15 coordinates which puts D into a given standard form for D. //

Actually the proof of Theorem (5.1) proves the stronger statement:

(5.2) Corollary: Given any two distinct copies D_1 and D_2 of a XNR-design, then there is a motion φ of the 16 coordinate places of $V(16,2)$ which fixes one coordinate and moves the other 15 coordinate places so that $D_1\varphi = D_2$.

(5.3) Theorem: The automorphism group of the unique XNR-design D is $A_7 + T(4)$, i.e. A_7 extended by $T(4)$, the group of the 16 translations of $V(4,2)$.

Proof: By Theorem (5.1), the design D is unique. As constructed in Theorem (5.3.9), this design D is composed of 7 orbits of dependent 6-sets under the action of $T(4)$, the translation group of $V(4,2)$. Hence, $T(4)$ stabilizes D. Since $T(4)$ is regular on $V(4,2)$, Lemma (3.2), any

motion of $T(4)$ fixing $\underline{O} \in V(4,2)$ is the identity vector. Then with $\underline{O}$ fixed, Lemma (2.1), Corollary (2.2), and Theorems (3.5) and (4.4) show that A_7 acts on D with $\underline{O}$ fixed. Hence, the total group of automorphisms D is A_7 extended by $T(4)$, $A_7 + T(4)$. //

(5.4) Theorem: The automorphism group $A_7 + T(4)$ of the XNR-design D is 1-transitive on the 112 blocks of the design.

Proof: By the construction method of D as shown in Theorem (5.3.9), $T(4)$ acting on D is $\frac{1}{2}$-transitive on blocks of D giving 7 orbits of 16 blocks each. Since $T(4)$ is regular on the 16 coordinate places of $V(16,2)$, by Lemma (3.2), there is always at least one block of each of these orbits which contains a 0 in the coordinate place of $V(16,2)$ corresponding to the $\underline{O} \in V(4,2)$. In other words at least one block of each of these orbits is contained in L . By Theorem (3.5) and Corollary (3.6), $Aut(L) \simeq A_7$ is 1-transitive on these 70 blocks. Therefore $A_7 + T(4)$ is 1-transitive on all the 112 blocks of D . //

(5.5) Theorem: $A_7 + T(4)$ is 3-transitive on the 16 points of X for the XNR-design $D = (x, \mathcal{B})$.

Proof: By Theorem (5.4), $A_7 + T(4)$ acts as a 1-transitive degree 112 group of permutations of the 112 blocks of D . Since each of the motions of $A_7 + T(4)$ is an automorphism of D , there is an isomorphic injection i mapping the group which acts on the 112 blocks of $\mathcal{B}$ into the group which acts on the 16 elements of X .

Let G be the subgroup of the action of $A_7 + T(4)$ on $\mathcal{S}$ which stabilizes a block $B \in \mathcal{B}$. Via the injection i, Gi is a homomorphic image of G on X stabilizing the two sets B and $X \setminus B$.

Claim: The homomorphic image Gi of G acting on the 6 elements of the stabilized block B gives a faithful representation of G on B.

Proof: Consider the mapping $\alpha : V(16,2) \to 2^{V(4,2)}$ for X being a basis of $V(16,2)$ which exists according to Theorem (7.5.1) in such a way that blocks of D are characteristic functions of dependent 6-sets in $V(4,2)$. Theorem (7.5.15) shows that each automorphism $\varphi \in Aut(D)$ induces a motion, $\alpha O_\varphi, \varphi$ followed by α, of $V(4,2)$ preserving linearity in $V(4,2)$. Then due to the fact that each dependent 6-set in $V(4,2)$ spans all of $V(4,2)$ by Lemma (4.5.8), it follows that if αO_φ fixes pointwise a dependent 6-set of $V(4,2)$, then αO_φ must fix pointwise all the 16 points of $V(4,2)$. Hence any motion of Gi fixing B pointwise induces the identity motion in the action Gi on X and hence is the identity automorphism of G. This proves the claim. //

Proceeding with the proof of Theorem (5.5) we notice that since G stabilizes one of the 112 blocks of $\mathcal{B}$, $|Gi| = 360$. Then the only subgroup of the set of all $6!$ permutations of the elements of B of this order is A_6. Hence $Gi \simeq A_6$, which is 4-transitive on the 6 points of B. As such, any triple of the 16 points of X may be

moved to any other triple of X by first moving one of the blocks through the first triple to one of the blocks through the other triple and then by using a motion of G on the image block. //

Note that the proof of Theorem (5.5) actually proves the following:

(5.6) Corollary: $A_7 + T(4)$ is 4-transitive on the set of $\binom{6}{4}.112$ 4-tuples contained in blocks of the XNR-design D.

CHAPTER 10

The Uniqueness of the Nordstrom-Robinson and The Extended Nordstrom-Robinson Binary Codes

§10.1 Introduction

This chapter will collect information from Chapters 5, 6, and 9 to show the uniqueness of the (15,256,5) code first discovered by Nordstrom and Robinson, together with the uniqueness of the extended (16,256,6) code. We shall use the notation NR and XNR for the (15,256,5) and (16,256,6) codes, respectively, according to Definition (3.5.8) and (3.5.4).

§10.2 The Uniqueness of the XNR(16,256,6) Code

(2.1) Theorem: Up to a permutation of the 16 standard basis vectors of V(16,2), the XNR(16,256,6) code is unique.

Proof: From Theorems (9.5.1) and (6.6.1) the code is unique up to a permutation of the 16 coordinate places. //

(2.2) Theorem: The automorphism group of the XNR(16,256,6) code is a degree 16 representation of the group $A_7 + T(4)$, i.e. A_7 extended by the group of translations of V(4,2), as long as $\underline{0} \in XNR$.

Proof: Given a particular copy of the unique XNR code, C, with $0 \in C$, then by Theorem (6.3.1), the set of 112 weight

6 vectors of C form an XNR-design D. By Theorem (9.5.2) this design D possesses the group $A_7 + T(4)$ as its group of automorphisms acting as a degree 16 group on the 16 standard basis vectors of $V(16,2)$. By the Definitions (5.2.5) and (5.2.6), the group of automorphisms of C must be a subgroup of $A_7 + T(4)$. But since Theorem (6.5.9) shows that the design D determines uniquely all the 256 vectors of C, each automorphism of D which by definition stabilizes the set D of weight 6 vectors of C must also stabilize the sets of weight 8, 10, 16, and 0 vectors of C. //

(2.3) Corollary: The group $A_7 + T(4)$ of automorphisms of the XNR(16,256,6) code is 3-transitive on the set of 16 standard basis vectors of $V(16,2)$.

Proof: Use Theorem (9.5.5). //

§10.3 The Uniqueness of the NR(15,256,5) Code

(3.1) Lemma: Given any two copies C_1' and C_2' of the XNR(16,256,6) code, then there is a motion φ which fixes one of the 16 coordinate places of $V(16,2)$, and permutes the other 15 so that $C_1'\varphi = C_2'$.

Proof: By Corollary (9.4.2) there is a φ fixing one coordinate place of $V(16,2)$ and permuting the other 15 places so that the weight 6 vectors of C_1', which form an XNR-design, D_1, are mapped onto the weight 6 vectors of C_2'. Then since each SNR-design D builds a (16,256,6) code in only one way by Theorem (6.5.9), the same φ maps C_1' to C_2'. //

(3.2) Theorem: The NR(15,256,5) binary code is unique up to a permutation of the 15 standard coordinate basis vectors of V(15,2).

Proof: Given any two (15,256,5) codes, C_1 and C_2, each extends by a parity check coordinate augmentation to a (16,256,6) code C_1' and C_2' respectively according to Definition (2.5.3) and Lemma (2.5.6). Now by Lemma (3.1) there is a permutation of the 15 coordinates of V(15,2) mapping C_1' and C_2' simultaneously C_1 to C_2'. //

§10.4 The Non-Linearity of the NR and XNR Codes

Using a simple idea due to J. M. Goethals [15] we can now show the non-linearity of both the unique NR(15,256,5) code and the XNR(16,256,6) code. As a by-product we have a distinct proof of the Calabi, et al. [7] result that there exists no linear (16,256,6) code.

(4.1) Theorem: The unique XNR(16,256,6) code is non-linear.

Proof: (J. M. Goethals) Let w.l.o.g. $\underline{0} \in C$, where C is a (16,256,6) code. By (6.3.1) the set of weight 6 vectors forms an XNR-design D. Choose any three coordinate places, $\underline{e}_1, \underline{e}_2$, and $\underline{e}_3$, from V(16,2). Since $b_3 = 4$ for the design D, there are exactly four vectors of weight 6 in C which contain ones in these three coordinate places. Call these four vectors $\underline{x}_1, \underline{x}_2, \underline{x}_3$, and $\underline{x}_4$. Then using the facts that $d \geq 6$ for all pairs of code vectors from C and since $|\underline{x}_i \cdot \underline{x}_j| \geq 3$ for each pair of these four vectors,

$i \neq j$, $i, j = 1,2,3,4$, then $|\underline{x}_1 + \underline{x}_2 + \underline{x}_3 + \underline{x}_4| = 12$. But according to Lemma (6.4.7), any (16,256,6) code C with $\underline{0} \in C$ contains no vector of weight 12. This implies that $\underline{x}_1 + \underline{x}_2 + \underline{x}_3 + \underline{x}_4 \notin C$ and that C is non-linear. //

(4.2) Corollary: The NR(15,256,5) code is non-linear.

Proof: By Definition (2.5.3) and Lemma (2.5.6) and by the uniqueness of the NR and XNR codes, the XNR code is necessarily the parity check code of the NR code. Similarly, by Definition (2.5.2) and Lemma (2.5.5) the NR code is necessarily the punctured code of XNR. Then by Lemmas (5.8) and (5.9) one code is linear iff the other is also linear. Hence, by Theorem (4.1), the NR code is non-linear. //

(4.3) Corollary: There exists no linear (16,256,6) code.

Proof: The (16,256,6) code is unique. //

PART D: THE GOLAY BINARY CODE

CHAPTER 11

The Uniqueness of the Large Steiner Systems S(4,7,23) and S(5,8,24)

§11.1 Introduction

As a by-product of our work with the uniqueness of the Nordstrom-Robinson code, we can show the uniqueness of the Steiner systems $S(4,7,23)$ and $S(5,8,24)$. Furthermore, we can show that the automorphism groups of these designs are of order $|M_{23}|$ and $|M_{24}|$, are block transitive on the designs, and are 4- and 5-transitive on the 23 and 24 point sets of those designs, respectively.

In an effort to locate a good setting for the action of the 4- and 5- transitive groups M_{23} and M_{24} discovered earlier by Mathieu [39], Witt (1938) showed in [40] the uniqueness of these Steiner systems building them up from the unique projective plane over $GF(5)$. Witt's concern was to establish the uniqueness of the 4- and 5- transitive groups M_{23} and M_{24}. Actually, H. Lüneborg [23] discovered and corrected a flaw in Witt's construction.

Much more recently, Jonsson built up the Steiner system $S(3,6,22)$ from facts concerning the geometry of $PG(3,2)$, cf. [19]. From the uniqueness of $S(3,6,22)$ thus established,

Jonsson concluded similar results about the uniqueness of the three large Steiner systems $S(3,6,22)$, $S(4,7,23)$, and $S(5,8,24)$ and their related automorphism groups M_{22}, M_{23}, and M_{24}. Our construction of these designs corresponds to constructing M_{23} from its maximal subgroup isomorphic to $A_7 + T(4)$ whereas that from Jonsson constructs M_{22} from S_6.

§11.2 The Uniqueness of S(4,7,23) Based on the Uniqueness of the XNR-Design

Throughout this section let X be a set of 23 points. Also let S be an $S(4,7,23)$ design.

(2.1) Lemma: $S = (X, \mathcal{B})$ is a 1-(4,7,23) design with $d \geq 8$ and each block B of $\mathcal{B}$ shares with 140 blocks of $\mathcal{B}$ three elements of B and with 112 blocks of $\mathcal{B}$ one element of B.

Proof: By definition, S is a $S(4,7,23)$ or a 1-(4-7-23) design so that each 4-tuple from X is contained in precisely one block of the design. Therefore, two distinct blocks share at most three elements of X and have Hamming distance $d \geq 8$ from one another.

By formulas (4.1.2) one sees that $b_0 = 253$, $b_1 = 77$, $b_2 = 21$, $b_3 = 5$, and $b_4 = 1$. Furthermore, $b_4 = 1$ implies $b^B_{5,0} = b^B_{6,0} = b^B_{7,0} = 1$ for a given block B of design S. Hence, the generalized block intersection numbers for S relative to a block B of the design are:

(2.2)

						253								
					176			77						
				120			56			21				
			80			40			16			5		
		52			28			12			4		1	
	32			20			8			4		0		1
16			16			4			4		0		0	1
0		16			0			4			0	0	0	1

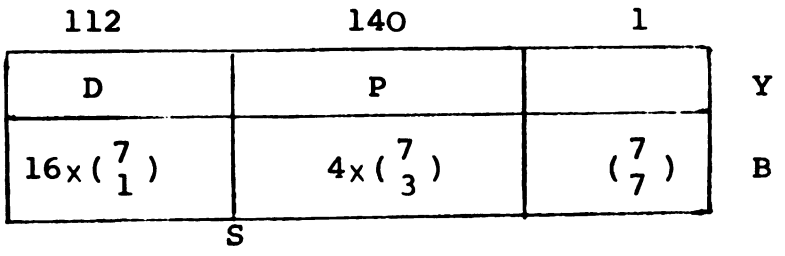
From the $b^B_{i,j}$ for $i + j = 7$ we conclude that each block B meets 4 blocks on each triple from B and 16 blocks on each element of B . Hence, B meets $\binom{7}{3} . 4 = 140$ blocks on three elements of B and $\binom{7}{1} . 16 = 112$ blocks on one element. //

Let $Y = X \setminus B$ be the set of the 16 points of S other than those of a fixed block.

(2.3) Lemma: The 140 blocks of S meeting B on 3 places form an S(3,4,16) design P on the 16 elements of Y . The 112 blocks of S meeting B on one place form an XNR-design D .

Proof: From the $b^B_{i,j}$ for S with respect to a block of S as given in (2.2), the 112 blocks of S meeting B in one place form, on the set B , 16 copies of the complete $\binom{7}{1}$-design. Similarly those 140 blocks meeting B on three places form on B four copies of the complete $\binom{7}{3}$-design. Let the corresponding parts of these 112 and 140 blocks with point set $y = X \setminus B$ be called designs D and P , respectively.

Figure (2.4)



Blocks of D have cardinality $k = 6$ since the corresponding weight 7 blocks of S meet B in one place.
Each 4-set from X occurs in a unique block of S, so that in D blocks have Hamming distance $d \geq 6$ from one another. Then for $t = 6 - 6/2 = 3$, equality in (4.7.5) holds showing by Lemma (4.7.7) and Definition (4.7.3) that D is an XNR-design. Design P is then a S(3,4,16) by the fact that each 4-tuple from Y occurs uniquely either in D or in P and by Definition (7.2.2) and Lemma (7.2.3). //

(2.5) Corollary: The 140 blocks of P as given in Figure (2.4) form the 140 planar 4-tuples of V(4,2) where the 16 vectors of V(4,2) are the 16 elements of Y.

Proof: This follows by Lemma (2.3) and Lemma (7.5.12). //

(2.6) Lemma: The 16 blocks of S through D meeting a fixed block B of S on a given single element of B form a 2-(2,6,16) design T with $d \geq 8$.

Proof: Consider the 16 blocks of S which meet B in precisely the element $x \in B$. Let T be the design whose point set is Y and whose blocks are those 16 blocks restricted to Y. Blocks of T have cardinality 6 and meet one another on 0 or 2 places since blocks of S meet one another on 1 and 3 places. Consider the average number of

blocks of T through any pair of points from Y . Formula (4.1.8) yields

$$\hat{b}_2 = 16.6.5/16.15 = 2 .$$

Since blocks of T meet on no more than 2 places, $b_2 = 2$ is a constant, so that T is a 2-(2,6,16) design with $d \geq 8$. //

(2.7) Lemma: Each block of the XNR-design, D , is contained in precisely one 2-(2,6,16) design, T , with $d \geq 8$ composed of 16 of the blocks from D . Thus the design D decomposes into a collection of 7 disjoint 2-(2,6,16) designs with $d \geq 8$.

Proof: That each block of D is in a 2-(2,6,16) design with $d \geq 8$ of 16 blocks of D is a result of Theorems 5.3.5) and (5.3.9). From the generalized block intersection numbers for D relative to a block, L , of D given in (6.4.6), $b^L_{2,4} = 1$ implies that there are precisely $1 \times \binom{6}{2} = 15$ other blocks of D that meet L in precisely two places, which blocks together with L could form a 2-(2,6,16) design, T , with $d \geq 8$. //

Now with these lemmas we can proceed to prove:

(2.8) Theorem: Up to a permutation of the 23 elements of X , the S(4,7,23) design S is unique.

Proof: Let S_1 and S_2 be any two S(4,7,23) designs defined on, for simplicity, the same point set X of cardinality 23. Choose any two blocks $B_i \in S_i$ for $i = 1,2$,

one from each design, and consider the corresponding subdesigns D_i and P_i of S_i, $i = 1,2$ as shown in Figure (2.4). Let $D_i = (X, \mathcal{B}_i)$ for $i = 1,2$. Because of Theorem (9.5.1) and Definition (5.2.1) there exists a pair of one to one correspondences (φ, ψ) for

(2.9) $\varphi : X \to X$ and $\psi : \mathcal{B}_1 \to \mathcal{B}_2$

so that (φ, ψ) map points and the blocks of D_1 to the points and blocks of D_2. We shall now proceed to show that each of the maps in the pair (φ, ψ) extend to the maps φ^* and ψ^* respectively in a unique way so that (φ^*, ψ^*) carry the points and blocks of S_1 to those of S_2 and so that

$$\varphi^* \mid_{X \setminus B_1} = \varphi \quad \text{and} \quad \psi^* \mid_{B_1} = \psi .$$

By Lemma (2.7), ψ maps each of the 2-(2,6,16) designs with $d \geq 8$ in D_1 to one of D_2. Since each block of D_i, $i = 1,2$, in a given 2-(2,6,16) design with $d \geq 8$ corresponds (Lemma (2.6)) to a single element of B_i, $i = 1,2$, there is a unique map

(2.10) $\Theta : B_1 \to B_2$

so that the combined map

(2.11) $\varphi^* \in S_{23}$, $\varphi : X \to X$

where

$$\varphi^* \mid_{X \setminus B_1} = \varphi \quad \text{and} \quad \varphi^* \mid B_1 = \Theta$$

carries points of S_1 to those S_2 at the same time that ψ carries the 112 blocks of S_1 meeting D_1 to the 112 blocks of S_2 meeting D_2.

Now that φ^* is defined it is sufficient in proving Theorem (2.8) to show that if the $23 \times (112+1)$ matrix part of S is given

Figure (2.12)

112	1	
D		$X \setminus B$
$16 \times \binom{7}{1}$	$\binom{7}{7}$	B

then the corresponding 140 blocks completing the design to an $S(3,7,23)$ are uniquely determined. (That the other 140 blocks are uniquely determined forces the extension ψ^* of ψ to be unique.)

(2.13) Claim: Given the 113 blocks of S as in Figure (2.12), then there is a unique way to complete these blocks to a $S(4,7,23)$ design.

Proof: Choose any three elements $a,b,c, \in X \setminus B$. These three elements are contained in blocks B_j, $j = 1,2,3,4$ of S meeting D and must be contained in one other block B_5 of S. Since $d \geq 6$ in D, $|\cup B_i| = 15$ and there is a unique 4-tuple from $X \setminus B$ containing $\{a,b,c\} \subset X \setminus B$. Since blocks B_j intersect one another in three elements, they are, by Lemma (2.7), members of distinct $2-(2,6,16)$ designs with $d \geq 8$. Then by Lemma (2.6) the corresponding single elements from B contained in the blocks B_j, $j = 1,2,3,4$, of S, must be distinct elements x_j, $j = 1,2,3,4$, of B. Then because in the $S(4,7,23)$ design S each 4-tuple must be contained in a unique block, the set of three elements of B contained in block B_5

must be $B \setminus \{x_j \mid j = 1,2,3,4\}$. So for each triple from $X \setminus B$ there is a unique block B_5 that necessarily must be chosen to complete the set of 113 blocks of Figure (2.12) to the design S . This finishes the proof of Theorem (2.8).//

(2.14) Corollary: In a $S(4,7,23)$ design S , the group of automorphisms stabilizing a block B of the design is $A_7 + T(4)$.

Proof: This follows from Lemma (2.3), Theorem (9.5.3), and the Claim (2.13). //

(2.15) Corollary: The $S(4,7,23)$ design exists and is unique.

Proof: Existence follows from Theorem (3.3.10) and Lemma (4.3.3). Uniqueness follows from Theorem (2.8).//

(2.16) Theorem: The automorphism group of $S(4,7,23)$ design S is block transitive.

Proof: Consider the set of 112 blocks of S meeting a fixed block B in one place. The stabilizer group of B is by Corollary (2.14) transitive on these 112 blocks. This means that given any two blocks B_1 and B_2 of S , if there is a third block B_3 meeting each of the first two blocks on one place each, then there is an automorphism of S moving B_1 to B_2 .

By the fact that any two blocks of S meet in either 1 or 3 places (Lemma (2.1)) we need only consider two cases. Let B_1 and B_2 be blocks of S .

Case 1: If $|B_1 \cap B_2| = 1$, then B_2 is one of

the 112 blocks meeting B_1 on one place. By the generalized block intersection numbers for the design D corresponding to these blocks, (cf. (6.4.6)) there are 36 blocks of D meeting B_2 on one place of the 16 point set $X \setminus B_1$ of D. Choose one of these 36 blocks and call the corresponding block of S, B_3. Since blocks of S meet one another on 1 or 3 places and since $|B_3 \cap B_2| = 1$, the single element of $B_2 \cap B_1$ must not be contained also in B_3. Hence, B_3 meets each of B_1 and B_2 on one place. Therefore there exists an automorphism of S stabilizing B_3 and moving B_1 to B_2.

Case 2: If $|B_1 \cap B_2| = 3$, then choose $a \in B_1 \setminus B_2$. There are 16 blocks of S meeting B_1 on only a and forming, with respect to $X \setminus B_1$, a 2-(2,6,16) design with $d \geq 8$. At most 4 of these 16 blocks share point a and three points of $B_2 \setminus B_1$, since each 4-tuple of X occurs in a unique block of S. So there are blocks of S meeting B_1 on a and B_2 on one place. Choose one of these, B_3. Then $|B_3 \cap B_2| = |B_3 \cap B_1| = 1$. Therefore again there is an automorphism of S fixing B_3 and moving B_1 to B_2. //

The group of automorphisms of S(4,7,23) is known to be M_{23} (cf. Witt [39]). We may conclude at this point the following:

(2.17) Corollary: The automorphism group of S(4,7,23) design S is of order $253.112.360 = 23.22.21.20.48 = |M_{23}|$.

Proof: Since Aut(S) is block transitive on 253 blocks of S by Theorem (2.16) and since the stabilizer group of a

block of S has order 112.360 by Theorem (9.5.3), Aut(S) has order 253.112.360. //

(2.18) Theorem: Aut(S) acts 4-transitively on the 23 points of S , where $S = (X, \mathcal{B})$ is the S(4,7,23) design.

Proof: Since Aut(S) is block transitive on $\mathcal{B}$ by Theorem (2.16), it suffices to show that the stabilizer of a block of S acts 4-transitively on the 7 points of that block. Choose a block $B \in \mathcal{B}$. Then by Corollary (2.14), the subgroup G of the action of Aut(S) on the 23 points of X stabilizing the sets B and $X \setminus B$ is isomorphic to $A_7 + T(4)$. G acts necessarily as an automorphism of the design P of Figure (2.4), since G must stabilize those blocks of S meeting block B in precisely 3 places. Furthermore, by Corollary (2.5), design P represents the set of 140 planar 4-tuples of a V(4,2) whose 16 vectors are the 16 elements of $X \setminus B$.

Choose a point $a \in X \setminus B$. Call the subgroup of G which fixes $a \in X \setminus B$ as well as stabilizes sets $X \setminus B$ and B , the group H . Then H must stabilize the 35 blocks of P which contain $a \in X \setminus B$. But the design of 35 blocks of P containing $a \in X \setminus B$ when restricted to the point set $X \setminus (B \cup \{a\})$ is the design of the 15 points and 35 lines of PG(3,2) , the derived design of the points and planar 4-tuples of V(4,2) . Therefore, H is a subgroup of the collineation group of PG(3,2) . By Theorem (9.5.3), Lemma (9.2.1), Theorem (9.3.5), and Theorem (9.4.4), in that order, $H \simeq A_7$. Therefore $H \simeq PSL(4,2)$ by Theorem (8.8.10) and acts on the

points and blocks of the derived design of P.

Choose any $\varphi \in H$ so that $\varphi \neq 1$, φ moves the 15 points of $X \setminus (B \cup \{a\})$ non-trivially. Since φ is a collineation of $PG(3,2)$, φ moves the 35 blocks of the derived design of P non-trivially.

Now since in S no two distinct blocks can contain the same 4-tuple from X, no two blocks of S meeting the derived design of P may contain the same triple $\{x,y,z\}$ from B, for then the two blocks would contain the same quadruple $\{a,x,y,z\} \subset X$. So the intersection of the 35 blocks of S meeting the derived design of P must form a complete $\binom{7}{3}$-design when restricted to the point set B (since all 35 triples thus obtained must be all the 35 distinct triples that are possible).

Since φ moves the 35 blocks of the derived design of P non-trivially, φ moves the 35 triples of the complete $\binom{7}{3}$-design non-trivially.

Finally, we notice that under the action of H, the set of 35 blocks of S passing through $a \in X \setminus B$ and through the derived design of P are stabilized. If φ were to fix the 7 elements of B, φ would also fix the 35 triples of the complete $\binom{7}{3}$-design stabilized by the action of H. Since φ moves these 35 triples non-trivially, φ also moves the 7 elements of B non-trivially.

Therefore that the action of H induces the faithful action of A_7 on the 7 elements of B. And since A_7 is 5-transitive on the 7 elements of B, this suffices to show that the stabilizer of a block of S is at least 4-transitive on the 7 elements of that block. //

§11.3 The Uniqueness of S(5,8,24)

Now that we have the fact that $S(4,7,23)$ is unique, we may proceed to show that a $S(4,7,23)$ design builds a $S(5,8,24)$ design in just one way (Theorem (3.9)). As such the $S(5,8,24)$ design will be shown to be unique (Corollary (3.10)).

Let X be a set of cardinality 23 and ∞ an additional element augmenting X to $X' = X \cup \{\infty\}$. Let S be a $S(4,7,23)$ design on X. In order to augment S to S' a $S(5,8,24)$, each block of S must be augmented by the extra point ∞ in order to obtain cardinality 8.

(3.1) Call these 253 new blocks of cardinality 8 extended blocks of S. The building of S' now concerns only the location of $506 = 759 - 253$ blocks of S' none of which contain ∞. For this reason we define:

(3.2) An admissible block of S' is a set of cardinality 8 on X which can be augmented to the set of extended blocks of S to form S'.

(3.3) Lemma: An admissible block S' meets 15, 168, and 70 extended blocks of S on 0, 2, and 4 places, respectively.

Proof: Let B be an admissible block of S' per Definition (3.2). Since no 5-tuple of X' may be contained in more than one block of S' , B may not meet any block of S in 5 or more places. Then considering the generalized block intersection numbers for S relative to B and using $b^B_{5,0} = b^B_{6,0} = b^B_{7,0} = b^B_{8,0} = 0$, one obtains:

(3.4)

253

176 77

120 56 21

80 40 16 5

52 28 12 4 1

33 19 9 3 1 0

21 12 7 2 1 0 0

15 6 6 1 1 0 0 0

15 0 6 0 1 0 0 0 0 .

From the bottom line we read that B meets $15.\binom{8}{0} = 15$ blocks of S in 0 places, $6.\binom{8}{2} = 168$ blocks in 2 places and $1.\binom{8}{4} = 70$ blocks in 4 places. //

(3.5) Lemma: The 15 blocks of S meeting an admissible block, B , of S' in no places form, when restricted to the set $X \setminus B$, a 3-(2,7,15) design, A . Furthermore, blocks of A meet one another in either 1 or 3 places.

Proof: Restricting the appropriate 15 blocks of S to the set $X \setminus B$ of cardinality 15 one sees that these 15 blocks have cardinality 7 each. They meet one another on either 1 or 3 places because they are contained in the design S all of whose blocks have that property (Lemma (2.1)). Then by Formula (4.1.8) we compute the average:

(3.6) $\hat{b}_2 = 15.7.6/15.14 = 3$.

Then since now two blocks meet in more than 3 places, all pairs must meet by (3.6) in exactly 3 places forcing this design, A , to be a 3-(2,7,15) design. //

(3.7) Lemma: The 70 blocks of S which meet an admissible block B of S' on 4 places form, when restricted to $X \setminus B$, a design M of whose blocks occurs twice. A duplicated triple of this S(3,4,15) design corresponds to two of the 70 blocks, which when restricted to B are complementary 4-tuples.

Proof: Let the design M be the set of 70 blocks of S meeting B in 4 places and restricted to the point set $X \setminus B$. Blocks of M are then triples from $X \setminus B$. Let L be any one of these triples from M . Since A as defined in Lemma (3.5) is a 3-(2,7,15) design, L is contained in 3 blocks K_3 , K_4 , and K_5 , of A . But L must be contained in precisely 5 blocks of S , so that these 5 blocks K_3 , K_4 , K_5 , and say K_1 and K_2 share pairwise exactly the set L and so that $\bigcup_{i=1}^{5} K_i = X$. Since $\bigcup_{i=3}^{5} K_i = X \setminus B$, L must be contained in two blocks of S which meet B in four places each, and these 4-tuples must be complementary. Therefore, L must occur twice as a block in M . //

(3.8) Corollary: An admissible block, B , of S' is the modulo 2 sum of blocks of S . which meet each other on three places, in 35 ways.

Proof: The design M contains 70/2 = 35 duplicated

triples. The corresponding 35 pairs of blocks each have B as their modulo 2 sum. //

(3.9) Theorem: A S(4,7,23) design S with point set X of cardinality 23 builds a S(5,8,24) design S' on the point set $X \cup \{\infty\}$ uniquely.

Proof: From Corollary (3.8) each admissible block of S' occurs as the modulo 2 sum of 35 pairs of blocks of S . But counting the maximal number of distinct admissible blocks of S' , we have $253.140/2 = 17710$ distinct pairs of blocks of S sharing 3 places (cf. Lemma (2.1)) and therefore $17710/35 = 506$ distinct admissible blocks. All of these must be used to form S' , and since S' exists (by Lemma (4.3.3)) all of these may be used to form S' . //

(3.10) Corollary: Up to a permutation of the 24 elements of the point set X' , the S(5,8,24) design S' is unique.

Proof: Let a S(5,8,24) design S' with point set X' be given. Upon choosing one of the elements, say ∞ , from X' , the 253 blocks containing ∞ form on $X = X' \setminus \{\infty\}$ a S(4,7,23) design S by (4.1.4). This design is unique up to a motion of the 23 elements of X by Theorem (2.7). Then by Theorem (3.9) this unique design builds S' uniquely.//

We actually have proved:

(3.11) Lemma: There is a permutation of the 24 elements of X' which fixes one element and maps any copy of S(5,8,24) onto any other. //

(3.12) Corollary: The S(5,8,24) design exists and is unique up to a permutation of its 24 points.

Proof: Use Lemma (4.3.3) and Theorem (3.9). //

(3.13) Theorem: The automorphism group of the S(5,8,24) design $S' = (X', \mathcal{B}')$ is of order 24.23.22.21.20.48 and acts transitively on its 759 blocks.

Proof: The stabilizer of a point of the 24 point set X' for S' has order $|M_{23}|$ by Corollary (2.16). Furthermore, the automorphism group acts transitively on the 24 points of X' since it is always possible to choose three points $a,b,$ and $c \in X'$ so that c is fixed and a permutation $\varphi \in S_{23}$ operating on the 23 points of $X' \setminus \{c\}$ may be found sending a to b and sending S' to itself by Lemma (3.11). Hence $|\mathrm{Aut}(S')| = 24.|M_{23}|$. //

(3.14) Corollary: $\mathrm{Aut}(S')$ acts 5-transitively on the 24 points of the design $S' = (X', \mathcal{B}')$.

Proof: The proof of Theorem (3.13) establishes the fact that $\mathrm{Aut}(S')$ is 1-transitive on the 24 points of X' . Since the stabilizer group of a point $\infty \in X'$ under the action of $\mathrm{Aut}(S')$ is an element of $\mathrm{Aut}(S)$ for the derived design S of S' , and since $\mathrm{Aut}(S)$ is 4-transitive on $X' \setminus \{\infty\}$ by Theorem (2.18), $\mathrm{Aut}(S')$ is 5-transitive on X' . //

CHAPTER 12

The Uniqueness of the GOLAY $(23,2^{12},7)$ and XGOLAY $(24,2^{12},8)$ Codes

§12.1 Introduction

Vera Pless has shown , in 1968, that any linear $(24,2^{12},8)$ code is necessarily the extended Golay code, [31]. However, her restriction of linearity is not necessary. From the uniqueness of the Steiner systems $S(4,7,23)$ and $S(5,8,24)$ established in the last chapter, and from ideas similar from those used in Chapter 6 relative to the Nordstrom-Robinson code, we shall demonstrate the uniqueness of the GOLAY $(23,2^{12},7)$ and the XGOLAY $(24,2^{12},8)$ codes. Said in other words, for the Golay binary codes, the number of code words M is less than or equal to 2^{12} with equality iff the codes are the GOLAY and XGOLAY codes defined in (3.3.5) and (3.3.8).

§12.2 The Weight Distribution of Any $(24,2^{12},8)$ Code

Let C be a $(24,M,8)$ code with $M = 2^{12}$. Let also $\underline{0} \in C$, where $\underline{0}$ is the all zero vector of length 24. We shall show that $M \leq 2^{12}$, (Lemma (2.1)). Equality for M implies that C has one vector each of weights 0 and 24 , 759 vectors of each of the weights 8 and 16, and 2576 vectors of weight 12, Theorem (2.12). Furthermore, the 759 vectors

of weight 8 necessarily determine a $S(5,8,24)$, Lemma (2.3).

(2.1) Lemma: Given C , any $(24,M,8)$ code, then $M \leq 2^{12}$.

Proof: Consider the code C_0 which is a punctured code of C . C_0 is then by (2.5.5) a $(23,M,7)$ code. By the sphere packing bound (3.2.3)

$$(2.2) \quad M \leq 2^{23}/(1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3}) = 2^{12}$$

where $e = \frac{7-1}{2} = 3$. //

(2.3) Lemma: Any $(24,2^{12},8)$ code C with $\underline{0} \in C$ has 759 weight 8 vectors which determine a $S(5,8,24)$ design.

Proof: Let C_0 be a punctured code of C . Then by (2.2), C_0 has its number M of code words satisfying equality in the sphere packing bound. So by Definition (3.2.4), C_0 is a perfect code. Therefore by Lemma (4.3.1), C_0 possesses 253 weight 7 code words determining a $S(4,7,23)$. Then by Lemma (4.3.2), C contains 759 weight 8 code words determining a $S(5,8,24)$ design. //

Within the proof of (2.3) we have the additional information:

(2.4) Corollary: Any $(23,2^{12},7)$ code C_0 , with $0 \in C_0$, is perfect and its weight 7 vectors determine a $S(4,7,23)$ design.

(2.5) Lemma: Any $(24,2^{12},8)$ code C , with $\underline{0} \in C$, possesses code words of weights 8, 12, and 16 .

Proof: By Lemma (2.3), C has 759 code words of weight 8. But this is true of any $(24,2^{12},9)$ code, C , with $\underline{0} \in C$, for example $C + \underline{z}$ where $\underline{z} \in C$. Consider now the coset code $C + \underline{z}$, where $\underline{z}$ is a code word of weight 8 of C .

The generalized block intersection numbers for the S(5,8,24) design determined by the 759 weight 8 vectors of $C + \underline{z}$ relative to a block L of the design (where L is determined by the code vector $\underline{z}$) are:

(2.6)

						759						
					506		253					
				330		176		77				
			210		120		56		21			
		130		80		40		16		5		
	78		52		28		12		4		1	
46		32		20		8		4		0		1
30	16		16		4		4		0		0	1
30		0		16		0		4		0	0	0	1

since each 5-tuple is contained in a unique block of S(5,8,24) forcing $b^L_{5,0} = b^L_{6,0} = b^L_{7,0} = b^L_{8,0} = 1$. One concludes from these generalized block intersection numbers that each block L meets $4x\binom{8}{4} = 280$ blocks on 4 places, $16x\binom{8}{2} = 448$ blocks on 2 places, and 30 blocks on 0 places. Therefore $\underline{z}$ meets 280 weight 8 code words of $C + \underline{z}$ at Hamming distance 8, 448 weight 8 code words at distance 12, and 30 weight 8 code words at distance 16. This means that in C there are code words of weight 0, 8, 12, and 16. //

(2.7) Lemma: If C is any $(24, 2^{12}, 8)$ code with $\underline{0} \in C$, then C contains no code words of weights 9, 10, or 11.

Proof: C possesses 759 code words of weight 8 forming a S(5,8,24) design, Lemma (2.3). If there exists a code word $\underline{z}_9$ of weight 9, then the 9-set A of X corresponding to $\underline{z}_9$ has $b^A_{5,0} = b_5 = 1$ showing that $\underline{z}_9$ meets some weight code vectors $\underline{x}$ on 5 places. This is impossible

because then the Hamming distance between $\underline{x}$ and $\underline{z}_9$ would be $7 < 8$. If $\underline{z}$ is a code word of weight 10 or 11 in C, then $\underline{z}$ must meet weight 8 code words in at most 5 places to maintain $d \geq 8$ in C. This means that the 10- or 11-set L corresponding to $\underline{z}$ meets blocks of the $S(5,8,24)$ design in at most 5 places. Now considering the generalized block intersection numbers for such a 10- or 11-set L, necessarily $b^L_{6,0} = b^L_{7,0} = b^L_{8,0} = b^L_{9,0} = b^L_{10,0} = 0$ and these numbers are:

759

506 253

330 176 77

210 120 56 21

130 80 40 16 5

78 52 28 12 4 1

33 19 9 3 1 0

12 7 2 1 0 0

6 6 1 1 0 0 0

6 0 1 0 0 0 0

-1 1 0 0 0 0 0 .

So necessarily $b^L_{4,6} \not\geq 0$ showing that $\underline{z}$ cannot have Hamming distance $d \geq 8$ with every weight 8 code vector. Hence, C contains no weight 9, 10, or 11 vectors. //

(2.8) Corollary: C contains no two code vectors located at distances 9, 10, or 11 from one another.

Proof: If $\underline{z}, \underline{x} \in C$ with $|\underline{z} + \underline{x}| = 9$, 10, or 11, then $C + \underline{z}$ would have a code word $\underline{z} + \underline{x}$ of weight 9, 10, or 11, contradicting Lemma (2.7). //

Define now

(2.9) an admissible weight 16 vector of C to a weight 16 vector V(4,2) which can be augmented to the set of 759 weight 8 vectors of C and yet preserve the distance $d \geq 8$ property.

(2.10) Lemma: An admissible weight 16 vector (cf. Definition (2.9)) of any $(24, 2^{12}, 8)$ code C with $0 \in C$ must be a complement of a weight 8 code word of C .

Proof: The point set X for the S(5,8,24) design S determined by the weight 8 vectors of C is the set of 24 standard basis coordinates of V(4,2) on which C is defined. Choose any admissible weight 16 vector of C . This determines a set L of 16 of the 24 points of X . Let L' be the complementary set to L , i.e. $L' = X \mid L$. Now consider the generalized block intersection numbers for S relative to this complementary set, L' :

												759											
										506				253									
								330				176				77							
						210				120				56			21						
				130				80				40				16		5					
			78				52				28				12			4		1			
		45+x				33-x				19+x				9-x				3+x		1-x		x	
	24+7x			21-6x				12+5x				7-4x				2+3x			1-2x		x-y		y
	-y			+y				-y				+y				-y			+y				
9+28x		15+21x				6+15x				6-10x				1+6x				1-3x		x-2y		y-z		z .
-8y+z		-7y-z				-6y+z				+5y-z				-4y+z				+3y-z		+z			

Now either $z = 1$ or 0, since $z = b_{8,0}^{L'}$ = the number of blocks meeting L' in all of its 8 places and is either a

block or not.

Suppose $z = 0$, then by $b^{L'}_{6,2} = x - 2y \geq 0$ and since $b^{L'}_{5,0} \geq b^{L'}_{6,0}$ implies $1 \geq x$, it is necessary that $y \leq \frac{1}{2}$. But since by Corollary (2.8) there exist no two vectors of C at distance 10 apart, $b^{L'}_{1,7} = 0$ implying that $15 + 7y = 21x$. Then noting that $b^{L'}_{5,3} \geq 0$, it is necessary that $1 - 15/7 - y + 3y \geq 0$ or $2y \geq 8/7$. This says that $y > \frac{1}{2}$ contradicting $y \leq \frac{1}{2}$. We may now only conclude that $z = 1$. This means that L' must be a code vector and that L must be a code vector and that L is the complement of a code word. //

(2.12) Lemma: Any $(24, 2^{12}, 8)$ code, C, with $\underline{0} \in C$ is complemented, i.e. the complement of any code word of C is again a code word.

Proof: Lemmas (2.5) and (2.10) ensure the existence in C of a code word, $\underline{z} \in C$, of weight 16, whose weight 8 complementary vector is also a code word. Considering the codes $C + \underline{z}$ and $C + (\underline{j} + \underline{z})$, one sees that, due to Lemma (2.3), there are 759 weight 8 code words in each of these coset codes. Therefore, $6 + \underline{z}$ contains $\underline{0} = \underline{z} + \underline{z}$, $\underline{j} = (\underline{j} + \underline{z}) + \underline{z}$, and 759 code words of each of the weights 8 and 16. By Lemma (2.10), those weight 16 code words in $C + \underline{z}$ must be the complementary vectors to the 759 weight 8 code words in $C + \underline{z}$. But $\underline{z} = \underline{0} + \underline{z} \in C + \underline{z}$, so that both $\underline{z}$ and $\underline{j} + \underline{z}$ are code words of $C + \underline{z}$ as well as of C. Then, since $C = C + \underline{z} + \underline{z}$, $j = (j + \underline{z}) + \underline{z} \in C$. So any $(24, 2^{12}, 8)$ code C with $\underline{0} \in C$, contains also $\underline{j}$ as a

code word.

Next, let $\underline{w}$ be any code word of C. The coset code $C+\underline{w}$ is a $(24,2^{12},8)$ code with $\underline{0} = \underline{w}+\underline{w} \in C+\underline{w}$, so $\underline{j} \in C+\underline{w}$. Therefore, $\underline{j}+\underline{w} \in C = C+\underline{w}+\underline{w}$. Hence, the complementary vector to any code word of C is also a code word of C. //

(2.13) Theorem: Any $(24,2^{12},8)$ code C, with $\underline{0} \in C$, has one code word of weights 0 and 24 each, 759 code words of weights 8 and 16, and 2576 code words of weight 12.

Proof: Since by Lemma (2.12) the complement of each code word is also a code word, and since C has 759 weight 8 vectors by Lemma (2.3), C has 759 weight 16 vectors complementary to those weight 8 vectors. Furthermore, C has $\underline{j} \in C$. The code words of weights $1,2,\ldots,7$ are impossible since $d \geq 8$ in C and $\underline{0} \in C$. Then by Lemmas (2.7) and (2.12), all other code words of C must be of weight 12. There are then $2^{12}-(1+759).2 = 2576$ weight 12 vectors in C. //

§12.3 The Designs S(4,7,23) and S(5,8,24) Build $(23,2^{12},7)$ and $(24,2^{12},8)$ Codes, Respectively, in One Way

By Chapter 11 we know that the designs $S(4,7,23)$ and $S(5,8,24)$ are unique up to a permutation of the point sets in question. Furthermore, by Lemma (2.3) and Corollary (2.4), each $(23,2^{12},7)$ and $(24,2^{12},8)$ code with $\underline{0} \in C$ contains weight 7 and 8 vectors which determine $S(4,7,23)$ and

S(5,8,24) designs, respectively. If we can show that each of these designs build the corresponding code in exactly one way, it will be shown that the corresponding codes are also unique. This is the goal of this section.

Let $S = (X, \mathcal{B})$ be a S(5,8,24) design, with X containing the 24 standard basis vectors of a V(24,2) as elements. Consider the set C of $1+759$ vectors of V(24,2) which are $\underline{0}$ and the 759 vectors of weight 8 whose 8 coordinate places containing ones from the 8-sets of the S(5,8,24) design. Define

(3.1) An admissible weight 12 vector to be a vector $\underline{z}$ of weight 12 from V(24,2) which has distance $d \geq 8$ from each of the 759 weight 8 vectors already in C. Let the 12-set given by the 12 coordinate places of an admissible weight 12 vector $\underline{z}$ containing ones be called an admissible 12-tuple of S.

(3.2) Lemma: An admissible 12-tuple L of S meets 132 blocks of S in 5 places, 495 blocks in 4 places, and 132 blocks in 2 places. These sets of blocks when restricted to the complementary 12-tuple $L' = X \setminus L$ form two copies of the complete $\binom{12}{2}$-design, the complete $\binom{12}{4}$-design, and an S(5,6,12) design, respectively.

Proof: Consider the generalized block intersection numbers for the design S relative to an admissible 12-tuple, L, of S. Such a 12-tuple meets blocks of 8 in at most 6 places, for otherwise the Hamming distance between the corresponding vectors would be less than 8. Hence,

$b^L_{j,0} = 0$ for $j = 7,8,\ldots,12$. Letting $b^K_{6,0} = x$, we see that the generalized block intersection numbers for 8 relative to the admissible 12-tuples L are:

759
506 253
330 176 77
210 120 56 21
130 80 40 16 5
28 52 28 12 4 1
45+x 33-x 19+x 9-x 3+x 1-x x
24 21 12 7 2 1 x 0
+7x -6x +5x -4x +3x -2x
9 15 6 6 1 1 x 0
+28x -21x +15x -10x +6x -3x
84x 15 35x 6 10x 1 x 0
-6 -56x -20x -4x
210x 22 70x 7 15x 1 x 0
-28 -126x -7 -35x -1 -5x
462x 38 126x 9 21x 1-6x x 0 0
-66 -252x -16 -56x -2
924x 66 210x 12 28x 1-7x x 0 0 0
-132 -462x -28 -84x -3

Since each $b^L_{0,8}$ and $b^L_{1,7}$ must be ≥ 0, $924x \geq 132$ and $66 \geq 462x$ showing that $x = 1/7$. Therefore the generalized block intersection numbers $b^L_{i,j}$ of S relative to L with $i + j = 12$ are $b^L_{i,j} = 0$ except for $b^L_{2,6} = 2$, $b^L_{4,4} = 1$, and $b^L_{6,2} = 1/7$. These numbers imply that L meets $1/7 \times \binom{12}{6} = 132$ blocks in 6 places, $1 \times \binom{12}{4} = 495$ blocks in 4 places and $2 \times \binom{12}{2} = 132$ blocks in 2 places. Since in S(5,8,24) each 5-tuple from X occurs in a unique block, the 132 blocks of S meeting L on 6 places must have the property, when restricted to the point set of L, that each 5-tuple is contained in a unique block. These 132

blocks then form a $S(5,6,12)$ design. A $S(5,6,12)$ design has by the formulas (4.1.2), $b_4 = 4$; the $S(5,8,24)$ has $b_4 = 5$. Therefore the set of 495 blocks of S meeting L on 4 places must form one copy of the complete $\binom{12}{4}$-design on L. Similarly $b_2 = 77$ in $S(5,8,24)$, $b_2 = 30$ in $S(5,6,12)$, and $b_2 = 45$ in the complete $\binom{12}{4}$-design. This implies that each pair from L must occur twice among the 132 blocks of S meeting L on two places, and that these pairs form two copies of the complete $\binom{12}{2}$-design when restricted to L.

According to Lemma (2.12), the set of 759+1 vectors of C may be completed to a $(24,2^{12},8)$ code only if the complementary vector to each code word is also a code word. Therefore the complementary 12-tuple to L, i.e. $L' = X \setminus L$ must also be an admissible 12-tuple. This means that L' meets blocks of S in the same manner as L does. //

(3.4) Theorem: Each admissible 12-tuple of S is the symmetric difference of two blocks of S which meet on two places in 66 ways.

Proof: Consider the dissection of $S = (X,\mathcal{B})$ into subdesigns according to an admissible 12-tuple $L \subseteq X$, as given in Lemma (3.2). Let sets A,B, and C be the sets of 132, 495, and 132 blocks of S which respectively meet L on 6, 4, and 2 places. Let $L' = X \setminus L$.

Consider the complete $\binom{12}{4}$-design of B restricted to L'. Let 1, 2, and 3 be three arbitrary points of L'. Since $b_3 = 9$ for a complete $\binom{12}{4}$-design (cf. 4.1.2),

$\{1,2,3\}$ is contained in 9 blocks of B.

Consider these 9 blocks of B containing $\{1,2,3\}$ and restrict attention to the set L. These 9 blocks form on L a design D of 12 points and 9 blocks. Design D has $d \geq 6$ since in $S(5,8,24)$ blocks have $d \geq 8$ and the parts of these 9 blocks of B restricted to L' differ pairwise in two places (i.e. have $d = 2$ when restricted to L'). Then D has $k = 4$ and $t = 4 - 6/2 = 1$ yielding equality in the formula (4.7.5)

$$b_0 \leq \lceil \frac{12-1}{4-1} \rceil \cdot \frac{12}{4} = 9 \quad .$$

Therefore by Lemma (4.7.6), D is a $3\text{-}(1,4,12)$ design. (Actually one can prove that D is the transpose of the affine geometry $AG(2,3)$ of two dimensions over $GF(3)$, but this is not necessary for our purposes.)

Let α be an arbitrary point of L. Since D has $b_1 = 3$, the set $\{\alpha,1,2,3\}$ is contained in precisely 3 blocks of B. Considering S, $b_4 = 5$, so $\{\alpha,1,2,3\}$ must also be contained in precisely two blocks of $C \cup A$. But blocks of A restricted to L' are pairs of points of L', so $\{\alpha 1,2,3\}$ is contained in two blocks of C.

Considering the complete $\binom{12}{4}$-design, E, and the two copies of the complete $\binom{12}{2}$-design, F, corresponding to blocks of B and C restricted to L', one calculates $b_1 = 165$ in E and $b_1 = 2 \times 11$ in F. Therefore $\{\alpha\}$ is contained in 165 blocks of B and 22 blocks of C.

Now considering b_2 for the designs G and H, $b_2 = 5$ in H. This implies that for an arbitrary pair $\{1,2,3\} \subset L'$, $\{\alpha,1,2\}$ is contained in 15+5 " 20 blocks of $B \cup C$. But $b_3 = 21$ in the S(5,8,24) design S, so that $\{\alpha,1,2\}$ must be contained precisely one block of A.

Restated, this last fact says that the pair $\{1,2\} \subset L'$, which is contained in precisely two blocks of A, is contained together with each $\alpha \in L$ in a unique block of A. This means that the two blocks of A containing an arbitrary pair $\{1,2\} \subset L'$, when restricted to the set L form complementary 6-tuples.

So we have finally shown that the admissible 12-tuple L is the symmetric difference (a modulo 2 sum) of two blocks of S which share a given pair from $L' = X \setminus L$. Furthermore, since there are 2×66 blocks of S in A and since there are 66 pairs in the complete $\binom{12}{2}$-design, any admissible 12-tuple L is the symmetric difference of two blocks of S in 66 ways. //

(3.5) Theorem: Given any S(5,8,24) design whose 24 point set X contains, as points, the 24 standard basis vectors of V(24,2), then S(5,8,24) always determines precisely one $(24,2^{12},8)$ code whose weight 8 vectors determine that S(5,8,24) design.

Proof: Let C be the set of 759 vectors of V(24,2) which have ones in the coordinate places corresponding to the elements of X in the 759 blocks of the S(5,8,24) design.

For C to be augmented to a $(24,2^{12},8)$ code, Theorem (2.13) requires there to be one vector of weights 0 and 24, 759 vectors of weights 8 and 16 and 2576 vectors of weight 12. By Lemma (2.12) the complement of each code word must also be a code word. Therefore we must augment C by $\underline{0}$, $\underline{j}$, and the 759 weight 16 vectors complementary to those already contained in C.

Now by Theorem (3.4), the only admissible weight 12 vectors are modulo 2 sums of two weight 8 vectors of C, each in 66 ways. By counting the maximum number of possible admissible weight 12 vectors we see that there are $759.448/2 = 170,016$ ways to choose pairs of blocks of S which share two elements of X. This yields $170.016/66 = 2576$ possible distinct admissible weight 12 vectors. All of these must be present in order to augment C to a $(24,2^{12},8)$ code.

Therefore, the $S(5,8,24)$ design builds a $(24,2^{12},8)$ code in a unique way. //

(3.6) Theorem: The $S(4,7,23)$ design builds a $(23,2^{12},7)$ code in a unique way.

Proof: Let Y be a 23 point set and $S = (Y,\mathcal{B})$ be a $S(4,7,23)$ design. Let ∞ be an additional point not from Y and let $X = Y \cup \{\infty\}$. By Theorem (11.3.9) the design S builds a unique $S(5,8,24)$ design on X. Let the 23 points of Y be the basis vectors of a $V(23,2)$ and ∞ be an additional vector so that points of X form a basis of

$V(24,2)$. Then by Theorem (3.5), the $S(5,8,24)$ design builds uniquely a $(24,2^{12},8)$ code C' on $V(24,2)$ whose weight 8 vectors determine that $S(5,8,24)$ design. Then a punctured code of this $(24,2^{12},8)$ code C' formed by removing the coordinate place corresponding to ∞ is a $(23,2^{12},7)$ code C , (cf. (2.5.5)), whose weight 7 vectors determine the $S(4,7,23)$ design S that was given.

Were S to be contained in any other copy of C_1 of a $(23,2^{12},7)$ code, then the parity check code, C_1' , $(24,2^{12},8)$ formed from C_1 would have its weight 8 vectors determining a distinct copy of the $S(5,8,24)$ (by Theorem (3.5)) and this would have (by Theorem (11.3.9)) a distinct $S(4,7,23)$ design as a derived design. This contradicts the fact that the punctured code of C_1' , namely C_1 itself, has its weight 7 vectors determining the same design S as the code C . Hence, S builds a unique $(23,2^{12},7)$ code C . //

§12.4 The Uniqueness of the GOLAY $(23,2^{12},7)$ and XGOLAY $(24,2^{12},8)$ Binary Codes

Since each $(23,2^{12},7)$ code and $(24,2^{12},8)$ code containing $\underline{0}$ has its minimum non-zero weight vectors determining respectively the unique $S(4,7,23)$ and $S(5,8,24)$ designs we have from Section 12.3 and Chapter 11 that:

(4.1) Theorem: Up to a permutation of the 23 basis vectors of $V(23,2)$, the GOLAY $(23,2^{12},7)$ code is unique. Up to a permutation of the 24 basis vectors of $V(24,2)$ the

XGOLAY $(24,2^{12},8)$ code is unique.

Proof: By Theorem (11.2.8) and Corollary (11.3.10) the $S(4,7,23)$ and $S(5,8,24)$ designs are unique up to a permutation of their 23 and 24 point sets respectively. Then by Theorems (3.6) and (3.5) these designs build unique $(23,2^{12},7)$ and $(24,2^{12},8)$ codes respectively. //

Furthermore, due to the fact that these Steiner systems build the respective codes in unique ways, we have:

(4.2) Theorem: The automorphism groups of the $(23,2^{12},7)$ and $(24,2^{12},8)$ codes containing $\underline{0}$ are isomorphic to the automorphism groups of the respective Steiner systems $S(4,7,23)$ and $S(5,8,24)$ determined by the minimum non-zero weight vectors of the codes. These automorphism groups are respectively 4- and 5-transitive on the 23 and 24 basis vectors of $V(23,2)$ and $V(24,2)$, while stabilizing these codes.

Proof: Use Theorems (3.6) and (3.5), and Theorems (11.2.18) and (11.3.14). //

BIBLIOGRAPHY

BIBLIOGRAPHY

1. E. Artin, The orders of the classical simple groups, Comm. Pure Appl. Math. 8(1955), 455-72.

2. E. F. Assmus and H. F. Mattson, On tactical configurations and error-correcting codes, Journal of Comb. Theory 3(1967), 243-257.

3. E. R. Berlekamp, Algebraic coding theory, McGraw Hill, New York, 1968.

4. E. R. Berlekamp, Coding theory and the Mathieu groups, Information and Control, 18(1971), 40-64.

5. F. C. Bussemaker and J. J. Seidel, Symmetric Hadamard matrices of order 36, Proc. Inter. Conf. Combin. Math., N. Y. Acad. Sci. (1970), 66-79.

6. F. C. Bussemaker and J. J. Seidel, Symmetric Hadamard matrices of order 36, Technological University Eindhoven, The Netherlands, T. H. Report 70-WSK-02, (1970).

7. L. Calabi and E. Myrvaagnes, On the minimal weight of binary group codes, Correspondence IEEE Trans. on Inform. Theory IT-10-4 (1964).

8. R. D. Carmichael, Introduction to the theory of groups of finite order, Dover Publ., New York, (1956).

9. J. H. Conway, A group of order 8,315,553,613,082,720,000, Bull. Lond. Math. Soc. 1(1969), 79-88.

10. G. M. Conwell, The three space PG(3,2) and its group, Ann. of Math., (2), 11(1910), 60-76.

11. P. Dembowski, Finite geometries, Berlin, Springer (1968).

12. P. Dembowski, Some characterizations of finite projective spaces, Arch. Math. 11(1960), 465-469.

13. L. E. Dickson, Linear groups, Dover Pub., New York, (1958), p. 309.

14. W. L. Edge, The geometry of linear fractional group LF(4,2), Proc. London Math. Soc. (3) 4(1954), 317-342.

15. J. M. Goethals, On the Golay perfect binary code, Journal of Comb. Theory, 11(1971), 178-186.

16. J. M. Goethals, On t-designs and threshold decoding, Univ. of North Carolina, Institute of Statistics Mimeo Series No. 600.29, June, 1970.

17. J. M. Goethals and S. L. Snover, Nearly Perfect Binary Codes, Discrete Mathematics, 3(1972), 65-88.

18. S. M. Johnson, A new upper bound for error-correcting codes, IRE Trans. Inform. Theory IT-8, (1962), 203-207.

19. W. Jonsson, On the Mathieu groups M_{22}, M_{23}, M_{24}, and the uniqueness of the associated Steiner systems, Math. Z., 125(1972), 193-214.

20. A. M. Kerdock, A class of low-rate nonlinear binary codes, Information and Control 20 no. 2 (1972), 182-187.

21. J. H. Van Lint, Coding theory, Lecture notes in mathematics, no. 201, Springer-Verlag, New York (1971).

22. C. L. Liu, B. G. Ong, and G. R. Ruth, A construction scheme for linear and non-linear codes, Discrete Mathematics, 4(1973), 171-184.

23. H. Lüneburg, Transitive Erweiterungen eindlicher Permutationsgruppen, Lecture notes in mathematics, no. 84, Springer-Verlag, New York (1969).

24. Mathieu, Journal de Mathematiques (1861), p. 270.

25. N. S. Mendelsohn, Intersection numbers of t-designs, Studie in pure mathematics, ed. L. Mirsky, New York, Academic Press (1971), 145-150.

26. D. M. Mesner, Sets of disjoint lines in PG(3,2), Canad. J. Math., 19 (1967), 273-280.

27. M. Nadler, A 32-point, n = 12, d = 5 code, IRE Trans. Inform. Theory IT-8 (1962), 58.

28. A. W. Nordstrom and J. P. Robinson, An optimum nonlinear code, Information and Control, 11(1967), 613-616.

29. L. J. Paige, A note on the Mathieu groups, Canad. J. Math., 9(1956), 15-18.

30. W. W. Peterson, Error-correcting codes, MIT Press, Cambridge (1961).

31. V. Pless, On the uniqueness of the Golay codes, Journal of Comb. Theory, 17(1968), 215-228.

32. F.P. Preparata, A class of optimum nonlinear double-error-correcting codes, Information and Control, 13(1968), 378-400.

33. J. Schönheim, On linear and nonlinear single-error-correcting q-nary perfect codes, Information and Control 12 (1968), 23-26.

34. A. Tietavainen and A. Perko, There are no unknown perfect binary codes, Ann. Univ. Turku, Ser. AI 148(1971).

35. J. A. Todd, Projective and analytical geometry, Sir Issac Pitman and Sons, Ltd., London (1958).

36. J. L. Vasil'ev and B. Lindström, On group and non-group perfect codes, Math. Scand. 25(1969), 149-158.

37. O. Veblen and J. W. Young, Projective geometry, Ginn and Co., New York (1918).

38. A. Wagner, On collineation groups of projective spaces I, Math. Z. 76(1961), 411-426.

39. E. Witt, Die 5-fach transitiven Gruppen von Mathieu, Abh. Math. Sem. Hamb. 12(1938), 256-264.

40. E. Witt, Uber Steinersche Systeme, Abh. Math. Sem. Hamb., 12(1938), 265-275.