Summer 2015

Uniquely clean elements, optimal sets of units and counting minimal sets of units

Brian Edward Borchers
University of Iowa

UNIQUELY CLEAN ELEMENTS, OPTIMAL SETS OF UNITS AND COUNTING MINIMALS SETS OF UNITS

by

Brian Edward Borchers

A thesis submitted in partial fulfillment of the
requirements for the Doctor of Philosophy
degree in Mathematics
in the Graduate College of
The University of Iowa

August 2015

Thesis Supervisor: Professor Victor Camillo

Graduate College
The University of Iowa
Iowa City, Iowa

CERTIFICATE OF APPROVAL

PH.D. THESIS

This is to certify that the Ph.D. thesis of

Brian Edward Borchers

has been approved by the Examining Committee for the thesis requirement for the Doctor of Philosophy degree in Mathematics at the August 2015 graduation.

Thesis Committee: _____
Victor Camillo, Thesis Supervisor

_____
Daniel Anderson

_____
Charles Frohman

_____
Richard Baker

_____
Oguz Durumeric

I dedicate this thesis to
my family and friends
with special thanks to
Victor Camillo

ACKNOWLEDGEMENTS

The following work continues an interest sparked while I was an undergraduate learning about eigenvectors.

I owe a great debt to my thesis adviser Vic who has worked with me over the past few years and helped edit and refine my thesis.

I also appreciate the support of my friends and family: my parents (Mark and Karen), my wife Mandy, my sons Ethan and Dylan, my siblings Amy, Daniel and Chad, numerous other relations; my good friends outside of school - Joey, Joe and Mark; John, Mark, Rebecca and many other classmates who helped me especially during my early years of graduate school and some of whom became good friends; and my program administrators and staff: Dan Anderson, Laurent Jay, Chris, Phyllis, Margaret and Cindy for their invaluable help during my time as a graduate student.

ABSTRACT

Let R be a ring. We say $x \in R$ is clean if $x = e + u$ where u is a unit and e is an idempotent ($e^2 = e$). R is clean if every element of R is clean. I will give the motivation for clean rings, which comes from Fitting's Lemma for vector spaces [3]. This leads into the ABCD Lemma, which is the foundation of a paper by Camillo, Khurana, Lam, Nicholson and Zhou.

Semi-perfect rings are a well known type of ring. I will show a relationship that occurs between clean rings and semi-perfect rings which will allow me to utilize what is known already about semi-perfect rings. [3] It is also important to note that I will be using the Fundamental Theorem of Torsion-free Modules over Principal Ideal Domains [6] to work with finite dimensional vector spaces. These finite dimensional vector spaces are in fact strongly clean, which simply means they are clean and the idempotent and unit commute. This additionally means that since $L = e + u$ for a linear transformation L, $Le = eL$

Several types of rings are clean, including a weaker version of commutative von Neumann regular rings, duo von Neumann regular. [7] The goal of my research is to find out how many ways to write matrices or other ring elements as sums of units and idempotents. To do this, I have come up with a method that is self contained, drawing from but not requiring the entire literature of Nicholson [8].

We also examine sets other than idempotents such as upper-triangular matrices and row reduced matrices and examine the possibility or exclusion that an element

may be represented as the sum of a upper-triangular (resp. row reduced) matrix and a unit. These and other element properties highlight some of the complexity of examining an additive property when the underlying properties are multiplicative.

PUBLIC ABSTRACT

A matrix is a rectangular array of numbers. Matrices occur commonly in all areas of pure and applied mathematics. Of the properties that matrices may have, being invertible or idempotent are among the most important. It is known that every square matrix is a sum of an invertible matrix and an idempotent matrix, this is called Fittings Lemma.

In this paragraph we abuse language a bit to communicate informally. This is a thesis in pure mathematics written in an applied mathematical spirit. It is, broadly thought of, an exercise in computing efficiency. We say a specific set of idempotents E generates all matrices if every matrix is a sum of an element in E and some invertible matrix. We are specifically interested in the so called $0, 1$ diagonal idempotents, (i.e. square matrices whose entries on the diagonal are 0 or 1 and entries off the diagonal are 0) the most important set in all of matrix theory. We ask the question, what is the smallest set of units required to generate all matrices with E? This number is hard to compute. For 2 by 2 matrices with entries in integers mod 3, the smallest number of units required is 32.

Specifically this thesis both computes and estimates. Our estimates actually yield a very interesting number in a limiting case and suggest quite an engaging but difficult conjecture. In our specific cases we obtain concrete numbers but the computations are quite technical. We also obtain a result for upper triangular matrices. You can think of an upper triangular matrix as a table in which all the entries in the

southwest corner are zero. Finally we study idempotents and so called row reduced matrices. These matrices are the foundation stone of the procedure used to solve systems of linear equations. In the 3 by 3 matrix case we do extensive computations to determine which matrices are the sum of a matrix from our distinguished set of diagonal idempotents and a row reduced matrix.

TABLE OF CONTENTS

CHAPTER

1 INTRODUCTION AND BACKGROUND 1

1.1 Introduction and Examples 1
1.2 Background and Motivation 3
1.3 von Neumann Regular Rings 6
1.4 Local Rings 8
1.5 Semi-perfect Rings 9
1.6 Morita Invariance 12

2 AN ESTIMATE FOR 2 BY 2 MATRICES 14

2.1 $Mat_2(Z/(p))$ 14
2.2 $Z/(p) \times Z/(p)$ 18
2.3 Conjectures 19

3 A FORMULA FOR COUNTING MINIMAL SETS 21

4 EXAMPLES FOR 2 BY 2 MATRICES 30

4.1 Diagonal Idempotent Unique Decompositions for $M_2(Z/(p))$ . . . 34
4.2 Optimal sets for $M_2(Z/(2))$ 35
4.3 Optimal sets for $M_2(Z/(3))$ 37

5 UNIQUE ELEMENTS FOR N BY N MATRICES 45

6 ROW REDUCED MATRICES 50

7 UPPER TRIANGULAR MATRICES 56

REFERENCES 59

CHAPTER 1
INTRODUCTION AND BACKGROUND

1.1 Introduction and Examples

Definition 1.1 Let R be a ring. We say $x \in R$ is *clean* if $x = e + u$ where u is a unit and e is an idempotent. [1] [2] [5] [7]

Example 1.2 Z has 4 clean elements.

Z has idempotents 0 and 1 and units 1 and -1. Therefore $0 + 1 = 1$, $0 + -1 = -1$, $1 + 1 = 2$ and $1 + -1 = 0$ are the clean elements.

A ring R is *clean* if every element in R is clean. Clean rings are widely studied. A Math.Sci.Net search yields 70 papers with the phrase "clean ring" in the title. This thesis is the initiation of a study of the number of ways the notion of clean can be implemented in specific situations.

Example 1.3 Let X be the non-negative natural numbers. Let B be the set $\{0, 1\}$. Then, $X = A_1 + B$ where the set A_1 of even non-negative integers is minimal for B in the sense that no subset B' of B has the property that $A + B' = X$. On the other hand $A_2 = \{0, 1, 3, 4, 6, 7, \dots\}$ is also a minimal set for B. It is easy to see that minimal sets for B all are sets A with the properties that: 1. A does not contain a sequence of three numbers. 2. For every number in X, either n is in A or $n - 1$ is in A.

Example 1.4 The notion of clean as a general abstract idea. Consider an object X that admits endomorphisms. As a set, denote these endomorphisms by $EndX$. Suppose that the identity is an endomorphism of X. Then we know that inverses are

defined in $EndX$. An idempotent is map which is the identity on its image, so if X contains images then we can talk about idempotents in $EndX$. This means that if addition is defined in $EndX$ (perhaps pointwise if X has addition) then the notion of a clean endomorphism is defined on X and a counting of the ways is appropriate.

Example 1.5 Linear Algebra. Consider $R = Mat_n(F)$, the ring of n by n matrices over a field F. Let D be the set of $\{0,1\}$ diagonal idempotents in R, i.e. diagonal matrices whose diagonal entries are either 0 or 1. If M is a matrix in R, there is a matrix E in D with $M - E$ invertible. To see this, note that by induction there is a $\{0,1\}$ diagonal idempotent $(n-1)$ by $(n-1)$ matrix E_1 that I can subtract from M_n (M_n removes the nth row and nth column from M) to create an invertible matrix U_1. We may extend E_1 to an n by n $\{0,1\}$ diagonal matrix in two ways, E_0 by adding a 0 and E_1 by adding a 1. It is clear that by expanding along the bottom row that if $det(M - E_0) = det(M - E_1) = 0$ then $det(U_1) = 0$ which is a contradiction. This also follows from Fitting's Lemma, but the above proof is more conceptual.

Example 1.6 Let R be a commutative von Neumann regular ring. Then R is clean. We will show a more general version later.

Example 1.7 Infinite motivation. Any infinite product of fields is von Neumann regular so is also clean as above. Suppose $R = \Pi F_i$ and for each F_i we have a set B_i which is minimal for $\{0,1\}$. Then ΠB_i is minimal for the set of all idempotents in R. This raises the question: which commutative von Neumann regular rings have sets that are minimal for their sets of idempotents?

1.2 Background and Motivation

In the context of the above we now discuss the notion of clean for background and motivation. Our work is very computational and finite so most of this background is not needed but it provides context.

Lemma 1.8

Fitting's Lemma [9]

Let V be a finite dimensional vector space and f be a linear transformation on V. Then there is an n with $V = Imf^{(n)} \bigoplus Kerf^{(n)}$.

Proof. There exists an n with

$$X = \bigcup_{i=1}^{n} ker(f^{(n)}) \qquad ker(f^{(n)}) = ker(f^{(n+1)})$$

$$Y = \bigcap_{i=1}^{n} Im(f^{(n)}) \qquad f^{(n)}(V) = f^{(n+1)}(V)$$

Claim 1: $V = X + Y$

Let $v, w \in V$ such that $f^{(n)}(v) = f^{(2n)}(w)$. Then $f^{(n)}(v - f^{(n)}(w)) = 0$ so $v - f^{(n)}(w) \in X$ and hence $v \in X + Y$.

Claim 2: $X \bigcap Y = 0$

Suppose $f^{(n)}(v) \in X$. Then $f^{(n)}(f^{(n)}(v)) = 0$. So $f^{(2n)}(v) = 0 \Rightarrow f^{(n)}(v) = f^{(n+1)}(v) = f^{(n+2)}(v) = \cdots = f^{(n)}(2v) = 0$.

This proves the claim.

We know by Claim 1 and Claim 2 that $V = X \bigoplus Y$. □

We now continue where we left off to set up motivation for the next lemma, using the same notation from the above lemma.

Claim: $f - \pi_X$ is monic. ($\pi_X : V = X \times Y \to V$ where $\pi_X(x, y) = x$)

Let $x \in X, y \in Y$. If $(f-\pi_X)(x+y) = 0$, then $f(x+y)-\pi_X(x+y) = f(x)+f(y)-x = 0$. Now, $f^{(n)}(x) = 0$ by definition of $x \in X$. As $ker(f^{(n+1)}(x)) = ker(f^{(n)}(x)) \Rightarrow (f^{(n)}(f(x)) = 0 \Rightarrow f(x) \in X$.

Let j be the minimum such that $f^{(j)}(x) = 0$. Now $f(x) = x \Rightarrow f(f(x)) = f(x) \Rightarrow \ldots \Rightarrow f^{(j-1)}(f(x)) = f^{(j-1)}(x)$. Which shows $x = f(x) = \cdots = f^{(j)}(x) = 0$. This proves the claim.

Since monics are epic, $f - \pi_X$ is a unit. Since we can always write $f = \pi_X + (f - \pi_X)$ and π_X is an idempotent this shows that a finite dimensional vector space has a clean endomorphism ring.

Note: f also commutes with π_X, as

$$\pi_X f(x + y) = \pi_X(f(x) + f(y)) = f(x)$$

$$f\pi_X(x + y) = f(x)$$

When f commutes with π_X, this is called strongly clean.

π_X is the motivation for the ABCD Lemma

Lemma 1.9

ABCD Lemma

Let $f \in End(M)$. Then f is clean $\iff$ there are subspaces A, B, C and D with

$$M = A \bigoplus B$$

$$M = C \bigoplus D$$

where $f\mid_A : A \to C, (1 - f)\mid_B : B \to D$ are isomorphisms.

Proof. $\Rightarrow$ Assume f is clean. Since f is clean, $f = e + u$ with the usual meaning.

Let $A = (1-e)M$, $B = eM$. So $M = (1-e)M \bigoplus eM = A \bigoplus B$.

Let $C = u(A),\ \ D = -u(B)$.

Then

$$\begin{aligned} (f)(a) &= (e+u)(1-e)(a) = (u)(1-e)(a) = (u)(a) \\ (1-f)(b) &= (1-f)(e)(b) = (1-e-u)(e)(b) = (-u)(b) \end{aligned}$$

Since f is clean, the decomposition exists and $f\mid_A$ and $(1-f)\mid_B$ are isomorphisms since u is a unit.

$\Leftarrow$ Assume

$$\begin{aligned} M &= A \bigoplus B \\ M &= C \bigoplus D \end{aligned}$$

where $f\mid_A \colon A \to C, (1-f)\mid_B \colon B \to D$ are isomorphisms.

Claim: $(f - \pi_B)$ is a unit where π_B denotes the usual projection.

Proof of Claim

Suppose $(f - \pi_B)(a+b) = 0$ where $a \in A$ and $b \in B$.

Then $f(a) + (f-1)(b) = f(a) - (1-f)(b) = 0$.

Since $M = C \bigoplus D$ and $f\mid_A$ and $(1-f)\mid_B$ are isomorphisms then $a = 0,\ \ b = 0$.

So we have shown $f - \pi_B$ is injective.

Also, consider given $c \in C$ and $d \in D$

$$\begin{aligned} c &= f(a) = (f - \pi_B)(a) \\ d &= (1-f)(b) = (\pi_B - f)(b) = -(f - \pi_B)(b) \end{aligned}$$

So we have shown $f - \pi_B$ is surjective. Thus the claim.

Since π_B is an idempotent, $f = \pi_B + (f - \pi_B)$ is the sum of an idempotent and a unit so f is clean. □

This is something that can be used in vector spaces in a very concrete way. Now we we explore a few different types of rings that are clean.

1.3 von Neumann Regular Rings

Definition 1.10 A ring R is *von Neumann regular* if for each $a \in R$ there exists an $x \in R$ with $a = axa$. [6]

Definition 1.11 A ring R is *right duo* if all maximal right ideals are also 2 sided ideals.

Lemma 1.12: right duo von Neumann regular rings are clean

If R is right duo von Neumann regular, then R is clean.

Proof. Let $a \in R$. Choose x with $a = axa$. Now rewrite a as

$a = (1 - xa) + a - (1 - xa)$.

Some useful facts that give context to the proof are given first.

Fact 1:

Since $(1 - xa)$ is an idempotent, we are done if we can show $a - (1 - xa)$ is a unit.

Fact 2:

$a - (1 - xa)$ is not right invertible iff $(a - (1 - xa)) \in M_R$ for each maximal right ideal M_R.

Claim 1: $a - (1 - xa)$ is right invertible

Proof of Claim 1

We shall prove this by contradiction. Suppose $(a-(1-xa)) \in M_R$ where M_R is a maximal right ideal.

Then

$$\begin{aligned}(a-(1-xa))xa &= axa - xa + xaxa \\ &= axa - xa + x(axa) \\ &= axa - xa + xa \\ &= axa \\ &= a \in M_R\end{aligned}$$

Right duo $\Rightarrow xa \in M_R \Rightarrow 1 \in M_R$ which is a contradiction to $M_R \neq R$.

So $a-(1-xa)$ is contained in no maximal ideal and hence $a-(1-xa)$ is right invertible.

Thus we have proved the Claim.

We now prove right invertible elements are also left invertible in a right duo ring.

Suppose $u \in R$ and u is right invertible, i.e. there exists $v \in R$ with $uv = 1$.

Claim 2: v has a right inverse.

Proof of Claim 2

We shall prove this by contradiction.

If v does not have a right inverse, $vR \subseteq M_R$ for some maximal right ideal M_R, i.e., $v \in M_R$. R right duo $\Rightarrow$ $uv = 1 \in M_R$ which is a contradiction.

So $vR = R$ which implies that there exists $r \in R$ such that $vr = 1$.

Thus the claim.

For all $r \in R$, since u has a right inverse we know $r = 1(r) = (uv)r = u(vr) = u(1) = u$ since v has a right inverse. So $r = u$. Thus u is also left invertible.

This shows that $a - (1 - xa)$ is a unit. □

Duo rings are not necessarily commutative. For an example, take any product of non-commutative fields.

Note. This is usually proved for commutative rings. However, the proof also works for the weaker requirement of duo rings.

1.4 Local Rings

In commutative algebra, a *local ring* is a Noetherian ring with a unique maximal ideal. A ring with a unique maximal ideal that may not be Noetherian is called *quasi-local*.

Lemma 1.13: Local Rings are clean

If R is a quasi-local (or local depending on context) ring, then R is clean.

Proof. Let $J = rad(R) = M$ where M is the unique maximal ideal. If $j \in J$, then $j = j - 1 + 1 = -(1 - j) + 1$

Since $j \in J$ we know $1 - rj$ is a unit for every $r \in R$. Thus $1 - j$ is a unit, so $-(1 - j)$ is a unit as well. Since 1 is an idempotent, j is clean.

If $u \notin J$, u is a unit and $u = u + 0$. □

1.5 Semi-perfect Rings

We present an informal discussion of this broad topic.

Lifting idempotents means if $x^2 + I = x + I$, (I a two sided ideal) (as cosets), then there exists $e \in R$ with $e^2 = e, i \in I$ with $x = e + i$. Further it is clear if $x = e + i$, then $x^2 - x \in I$ since $x^2 - x = (e+i)^2 - (e+i) = ei + ie + i^2 - i \in I$ $(x + I = e + I)$ This is not that surprising as R/I is a ring. What is surprising is that if I is only 1-sided, Nicholson discovered that idempotents will lift mod I if the ring is clean [8] [4]. I am going to show some calculations that are very important. They will show that clean $\Rightarrow$ exchange and that I-finite clean is a Morita invariant. I-finite means there are no infinite sets of orthogonal idempotents.

Now, let x be a clean element, so now we can write $x = e + u$, $e^2 = e$, u is a unit. So $x^2 - x = ue + eu + u^2 - u$.

First we multiply on the right by u^{-1}

$$1) \qquad (x^2 - x)u^{-1} = ueu^{-1} + e + u - 1,$$

Since $x = e + u$ and $uu^{-1} = 1$ we can rewrite this as

$$1a) \qquad (x^2 - x)u^{-1} = x - u(1 - e)u^{-1}$$

(this shows every non-zero right ideal contains a non-zero idempotent if $e \neq 1$)

moving and factoring x yields

$$\begin{aligned} x - x(x-1)u^{-1} &= u(1-e)u^{-1} \\ x(1 - (x-1)u^{-1}) &= u(1-e)u^{-1} \end{aligned}$$

Therefore $u(1-e)u^{-1} = f \in xR$ where f is idempotent.

Now we start again using 1)

$$(x^2 - x)u^{-1} + 1 - x = ueu^{-1} \quad = \quad g$$

$$(1-x)(1-xu^{-1}) = g \quad = \quad 1 - f$$

$\therefore\ 1 - f \in (1-x)R.$

There is a module theory of exchange in Lam [6], but we are going to use the following as it suits our purposes.

Definition 1.14 R is *exchange* if for every $x \in R$ there exists $e \in R, e^2 = e$ such that $e \in xR$ and $(1-e) \in (1-x)R$.

Theorem 1.15 If R is clean, then R is exchange.

Proof. Using the equations above we showed $f \in xR$ and $1 - f \in (1-x)R$

So clean rings are exchange [3]. □

(So one equation says idempotents lift mod one sided ideals and clean implies exchange.)

Using 1a) we now write

$$2) \qquad\qquad x \equiv f\ mod(x^2 - x)$$

If x is an idempotent $mod(A_R)$ where A_R is a right ideal, this is the same as $x^2 - x \in A_R$

Now by 2), $x - f \in A_R \ \Rightarrow\ x \equiv f\ mod(A_R)$. So idempotents lift mod right ideals.

Theorem 1.16 Let R be a clean ring with $J = 0$ where J denotes the Jacobson radical of R. Then every non-zero right ideal contains a non-zero idempotent.

Proof. Let $y \neq 0 \in R$. By properties of the Jacobson radical, we know $1 - yr$ is not a unit for some $r \in R$. Let $x = yr = e + u$, then $e \neq 1$, or else $1 - x = 1 - yr$ is a unit. By previous computations, we know $u(1-e)u^{-1} \in yR$. As $e \neq 1 \Rightarrow u(1-e)u^{-1} \neq 0$. $\square$

Definition 1.17 R is *semi-perfect* if R/J is Artinian and idempotents lift mod J.

Lemma 1.18

$$\text{If } R = \bigoplus_{i=1}^{n} e_i R \text{ where each } e_i R \text{ is indecomposable and } e_i^2 = e_i$$

$$\text{then } R \text{ is clean} \Leftrightarrow R \text{ is semi-perfect.}$$

Proof. $\Leftarrow$ Suppose R is semi-perfect. We know R/J is clean by Wedderburn's Theorem and Fitting's Lemma.

Let $x \in R$ and use $\bar{}$ to denote mod J.

Then $\bar{x} = \bar{a} + \bar{u}$ and since $(\bar{a})^2 = \bar{a} \Rightarrow a^2 - a \in J$. Since idempotents lift mod J, there is an idempotent e and $j_1 \in J$ with $a = e + j_1$. Now $\bar{x} = \bar{a} + \bar{u} \Rightarrow x = a + u + j_2$; with $j_2 \in J$, so $x = e + j_1 + j_2 + u$. Let M be a maximal ideal. If $j_1 + j_2 + u \in M$, since $j_1 + j_2 \in J \subseteq M \Rightarrow u \in M$ which is a contradiction. This implies $j_1 + j_2 + u$ is a unit. So x is clean.

$\Rightarrow$ Suppose R is clean.

$$R = \bigoplus_{i=1}^{n} e_i R \text{ ; } e_i R \text{ are indecomposable and } e_i^2 = e_i$$

Our previous work showed idempotents lift mod right ideals, so we know idempotents lift mod J. In order to show R is semi-perfect, it remains to show R/J is semi-simple.

Claim: R/J is clean

$x = e + u \Rightarrow \bar{x} = \bar{e} + \bar{u}$ and since $(\bar{e})^2 = \bar{e}$ and $\bar{u}$ remains a unit.

This proves the claim.

Claim: $\bar{e_i}\bar{R}$ is a simple module.

Proof by contradiction.

Suppose $\bar{e_i}R \supset \bar{y}R \neq 0 \Rightarrow \bar{y}R$ contains a non-zero idempotent f.

$\Rightarrow \bar{R} = \bar{f}\bar{R} \bigoplus (\overline{1-f})\bar{R}$.

(Now modularity tells us that for any module M: if $M = x \bigoplus y$ and $x \subseteq z$ then $z = x \bigoplus (z \cap y)$.)

Since $\bar{e_i}R \supset \bar{f}R \neq 0$

by modularity we get $\bar{e_i}R = \bar{f}R \bigoplus (\bar{e_i}R \cap (\overline{1-f})R)$ and $\bar{e_i}R \cap (\overline{1-f})R \neq 0$

$\Rightarrow \bar{e_i}R$ is decomposable, a contradiction. Thus the claim.

So R/J is the finite sum of simples and thus semi-simple. So R is semi-perfect. $\square$

1.6 Morita Invariance

Since semi-perfect is a Morita invariant, I-finite + clean is a Morita invariant. It is known that matrix rings over clean rings are clean. But, if a matrix ring over a ring is clean, it is not known if the ring is clean.

Note 1: I-finite implies the condition needed by Lemma 1.18 above.

Note 2: von Neumann regular and semi-simple are Morita invariants, but commutative and local are not.

Note 3: Two rings R and S are Morita equivalent if M_R and M_S are equivalent as categories.

Example 1.19 Any ring R with 1 is Morita equivalent to any matrix ring $M_n(R)$ over it.

CHAPTER 2
AN ESTIMATE FOR 2 BY 2 MATRICES

Recall that a ring R is clean if every element of R is a sum of a unit and an idempotent. We investigate minimal sets that make this decomposition possible.

Definition 2.1 Let R be a ring. A set of idempotents E in R is called *beautiful* if $E + Units(R) = R$.

Definition 2.2 A set of units U is said to be *attractive* for a set of idempotents E if $U + E = R$.

Example 2.3 Consider $Z/(p)$ for a prime p. Let $E = \{0, 1\}$.

Then $V = \{1, 3, 5, 7, \ldots, p-2, p-1\}$ is a set of units that is attractive for E. Note that $\mid V \mid = \frac{p+1}{2}$.

Throughout this paper p will always be a prime.

2.1 $Mat_2(Z/(p))$

Let $R = Z/(p)$. We consider $Mat_2(R)$. Let F be the $\{0, 1\}$ diagonal idempotent matrices. We now will find a set of units that is attractive for F.

First let X be the diagonal matrices in $Mat_2(R)$. X is an additive subgroup of $M_2(R)$. X has cardinality $|X| = p^2$. So as an additive subgroup X has index $\frac{p^4}{p^2} = p^2$.

We find a set of additive coset representatives for X that are units. These fall into four classes:

1)

$$\mathcal{A} = \left\{ \left[\begin{array}{cc} 0 & b \\ c & 0 \end{array} \right] \middle| \, b, c \neq 0 \right\}$$

then $|\mathcal{A}| = (p-1)^2$

2)

$$\mathcal{B} = \left\{ \left[\begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right] \middle| \, x \neq 0 \right\}$$

then $|\mathcal{B}| = (p-1)$

3)

$$\mathcal{C} = \left\{ \left[\begin{array}{cc} 1 & 0 \\ y & 1 \end{array} \right] \middle| \, y \neq 0 \right\}$$

then $|\mathcal{C}| = (p-1)$

4)

$$\mathcal{D} = \left\{ \left[\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right] \right\}$$

and $|\mathcal{D}| = 1$

Then

$$\begin{aligned} |\mathcal{A}| + |\mathcal{B}| + |\mathcal{C}| + |\mathcal{D}| &= (p-1)^2 + 2(p-1) + 1 = p^2 - 2p + 1 + 2p - 2 + 1 \\ &= p^2 \end{aligned}$$

which is the index of X in R.

We note that none of $T = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C} \cup D$ can be obtained from the other by the addition of a diagonal. So T contains one additive coset representative for cosets mod X.

Consider a coset with representative $U_0 = \left[\begin{array}{cc} 0 & b_0 \\ c_0 & 0 \end{array} \right]$ with $b_0 \neq 0, c_0 \neq 0$.

Recall V from Example 2.3. Let $W = \begin{bmatrix} v_1 & 0 \\ 0 & v_2 \end{bmatrix}$ with $v_1, v_2 \in V$ and F is the set of $\{0, 1\}$ diagonal matrices.

Every matrix J in the coset $U_0 + X$ is of the form:

$J = (U_0 + W_0) + F_0, W_0 \in W, F_0 \in F.$

We want to estimate the number of units we need to get the elements in $U_0 + X$.

It would be nice if $\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} + \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}$ is a unit but this is not true in general since,

if $det(\begin{bmatrix} x & b \\ c & y \end{bmatrix}) = 0$ (i.e. ,$y = x^{-1}bc$) then the sum is not a unit.

Now, there are $(\frac{p+1}{2})^2$ elements in W and at most $\frac{p+1}{2}$ of the form $\begin{bmatrix} x & 0 \\ 0 & x^{-1}bc \end{bmatrix}$ since these are determined by x when $x \in V$ and $x^{-1}bc \in V$.

So suppose $J = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} + \begin{bmatrix} x & 0 \\ 0 & x^{-1}bc \end{bmatrix} + F_0$

Then if $F_0 = \begin{bmatrix} 1 & 0 \\ 0 & g \end{bmatrix}$ we write

$J = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} + \begin{bmatrix} x+1 & 0 \\ 0 & x^{-1}bc \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & g \end{bmatrix}$ where the sum of the first two terms is a unit. There are $\frac{p+1}{2}$ of them, one for each x.

We do the same thing for $F_0 = \begin{bmatrix} h & 0 \\ 0 & 0 \end{bmatrix}$.

If $h = 1$ we have already solved our problem above, so we create $\frac{p+1}{2} - 1$ new units.

If $F_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$,we create one new unit:

$$J = \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} + \begin{bmatrix} x-1 & 0 \\ 0 & x^{-1}bc \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Adding and subtracting these amounts we get

$$\begin{aligned} \left(\left(\frac{(p+1)}{2}\right)^2 - \frac{p+1}{2}\right) + \left(\frac{p+1}{2}\right) + \left(\frac{p+1}{2} - 1\right) + 1 &= \left(\tfrac{(p+1)}{2}\right)^2 + \left(\tfrac{p+1}{2}\right) \\ &= \left(\tfrac{p+1}{2}\right)\left(\tfrac{p+1}{2} + 1\right) \\ &= \left(\tfrac{p+1}{2}\right)\left(\tfrac{p+3}{2}\right) \\ &= \tfrac{(p+3)(p+1)}{4} \end{aligned}$$

Now that we know this we are ready to compute the overall number of units needed for all the cosets.

For each coset in $\mathcal{A}$ we require $\left(\frac{(p+3)(p+1)}{4}\right)$ units and there are $(p-1)^2$ such cosets, so for $\mathcal{A}$ we may require $\left(\frac{(p+3)(p+1)(p-1)^2}{4}\right)$ units.

For each coset in $\mathcal{B}$ we require $\left(\frac{p+1}{2}\right)$ units and there are $(p-1)$ such cosets, so for $\mathcal{B}$ we may require $\left(\frac{(p+1)(p-1)}{2}\right)$ units.

For each coset in $\mathcal{C}$ we require $\left(\frac{p+1}{2}\right)$ units and there are $(p-1)$ such cosets, so for $\mathcal{C}$ we may require $\left(\frac{(p+1)(p-1)}{2}\right)$ units.

For each coset in $\mathcal{D}$ we require $\left(\frac{p+1}{2}\right)$ units and there are 1 such cosets, so for $\mathcal{D}$ we may require $\left(\frac{p+1}{2}\right)$ units.

So we know we can find the following units $U(p)$ that are attractive for F in

$Mat_2(R)$ with

$$\begin{aligned}
|U(p)| &= \left(\frac{(p+3)(p+1)(p-1)^2}{4}\right) + 2\left(\frac{(p+1)(p-1)}{2}\right) + \left(\frac{p+1}{2}\right) \\
&= \left(\frac{(p^2+4p+3)(p^2-2p+1)}{4}\right) + 4\left(\frac{(p+1)(p-1)}{4}\right) + 2\left(\frac{p+1}{4}\right) \\
&= \left(\frac{p^4+2p^3-4p^2-2p+3}{4}\right) + \left(\frac{4p^2-4}{4}\right) + \left(\frac{2p+2}{4}\right) \\
&= \left(\frac{p^4+2p^3+1}{4}\right)
\end{aligned}$$

Since there are p^4 elements in $M_2(R)$ we now compute the limit as p approaches infinity of the ratio of the units required ($|U(p)|$)to the total elements in $M_2(R)$ (p^4) which is

$$\begin{aligned}
lim_{p\to\infty}\frac{\left(\frac{p^4+2p^3+1}{4}\right)}{p^4} &= lim_{p\to\infty}\frac{\frac{p^4+2p^3+1}{4p^4}}{\frac{p^4}{p^4}} \\
&= lim_{p\to\infty}\frac{\left(\frac{1+\frac{2}{p}+\frac{1}{p^4}}{4}\right)}{1} \\
&= \frac{\frac{1}{4}}{1} \\
&= \frac{1}{4}
\end{aligned}$$

Definition 2.4 $\lceil x \rceil$ is the ceiling function of x.

So our estimate for the cardinality of an attractive set of units is $\frac{1}{4}$ of the total elements for $Mat_2(R)$. It should be noted that this is also surprising since the minimum number of units needed is $\lceil \frac{p^4}{4} \rceil$.

2.2 $Z/(p) \times Z/(p)$

Now consider the ring $Z/(p) \times Z/(p)$.

Let E be the set of idempotents $\{(0,0),(0,1),(1,0),(1,1)\}$. Recall V from Example

2.3. Since there are no matrix issues here it is clear that there are $\left(\frac{(p+1)}{2}\right)^2$ units ($|U(p)|$) that are attractive for E. Then computing the limit as p approaches infinity of the ratio of the units required ($|U(p)|$)to the total elements in $Z/(p) \times Z/(p)$ (p^2) we get

$$\begin{aligned} lim_{p\to\infty}\frac{|U(p)|}{|Z/(p)\times Z/(p)|} &= lim_{p\to\infty}\frac{\left(\frac{(p+1)}{2}\right)^2}{p^2} \\ &= lim_{p\to\infty}\frac{\frac{(p^2+2p+1)}{4}}{p^2} \\ &= lim_{p\to\infty}\frac{\frac{(p^2+2p+1)}{4p^2}}{\frac{p^2}{p^2}} \\ &= lim_{p\to\infty}\frac{\frac{(1+\frac{2}{p}+\frac{1}{p^2})}{4}}{1} \\ &= \frac{\frac{1}{4}}{1} \\ &= \frac{1}{4} \end{aligned}$$

So this is evidence that only the entries on the diagonal of a matrix matter when computing the set of units required. This leads us to the following conjectures.

2.3 Conjectures

Conjecture 1

Let $R = Mat_n(Z/(p))$ and let E be the $\{0,1\}$ diagonal idempotent matrices.

The ratio of the units required ($|U(p)|$)to the total elements in $M_n(Z/(p))$ is

$lim_{p\to\infty}\frac{|U(p)|}{|R|} = \frac{1}{2^n}$

Conjecture 2

Let R be a finite field and let E be the $\{0,1\}$ diagonal idempotents in $M_n(R)$.

The ratio of the units required ($|U(R)|$)to the total elements in $M_n(R)$ is

$lim_{|M_n(R)|\to\infty} \frac{|U(R)|}{|M_n(R)|} = \frac{1}{2^n}$

CHAPTER 3
A FORMULA FOR COUNTING MINIMAL SETS

In general it is hard to compute cardinalities of optimal and minimal sets which is why we earlier started with an estimate for $M_2(Z/(p))$. However, certain types of rings that are finite have a nice structure which allows us to not just compute cardinalities, but also determine the form of minimal sets and count all possible ways that these minimal sets can occur.

Let $R = Z/(p)$, let $E = \{0, 1\}$ and let A be the units of R, i.e., $A = \{1, 2, \cdots, p-1\}$ where we write a for $\bar{a}$ for all $a \in A$.

We know that there exists $B \subseteq A$ such that $B + E = R$.

Definition 3.1 B is *minimal* if there does not exist $C \subset B$ with $C + E = R$.

This is to say that B is minimal if the removal of any element will mean that some element in R will not be able to be expressed. There may exist D such that $|D| < |B|$ but $D \not\subset B$ and $D + E = R$. So it is possible that there may exist other sets with lower cardinality that are also minimal, but they cannot be obtained by removing elements from a minimal set.

Definition 3.2 A set is *optimal* if it is a minimal set with the lowest possible cardinality.

Recall that $\lceil x \rceil$ means the ceiling function of x.

Theorem 3.3

Let $R = Z/(p)$ where p is an odd prime. Let $E = \{0, 1\}$.

Let d be the number of possible minimal sets of units with respect to E.

Then $d = \sum_{i=0}^{i<\lceil \frac{p-3}{6} \rceil} \binom{\frac{p-1}{2}-i}{2i+1}$.

Proof. We begin by discussing what a minimal set B can or can't look like. Every minimal set must contain 1 and $p-1$. This is because 0 is not a unit and therefore the only way to generate the element 1 is to use 1 and the idempotent 0 and the only way to generate 0 is to use $p-1$ and the idempotent 1. Also, a minimal set may never contain 3 consecutive elements, $a, a+1, a+2$ since $a+1$ could be removed and the same elements of R, namely $a, a+1, a+2, a+3$ could still be generated. Therefore a minimal set must contain sequences of the form a or $b, b+1$ where the former will be referred to as a singleton and the latter as a pair and $a-1$, $a+1$, $b-1$, $b+2 \notin B$. Conversely, a minimal set may never omit two consecutive units. This is to say that if $a, a+1 \notin B$, then it is not possible for $a+1$ to be generated, thus B would not be minimal, a contradiction. Therefore it is only allowed to omit one unit between a singleton or a pair. Now since p is odd, this means that $p-1$ is even. This fact forces every minimal set to contain at least one pair. This is due to the fact that a minimal set must start with an odd number (1) and end with an even $(p-1)$. It is clear that if c is the next element being chosen in B that c is odd (resp. even) if the previous element a is odd (resp. even). Thus to change from odd to even we must have at least one pair. An even number of pairs is not possible since it would force us to end on an odd, but we must end on an even. Therefore we know that we must always have an odd number of pairs with a minimum of one pair.

An optimal set is therefore a minimal set that contains only 1 pair. The

cardinality of an optimal set is precisely $\frac{p+1}{2}$ since we have $\frac{p-3}{2}$ singletons and 1 pair. This becomes the basis for our following deductions and the base case for the formula. $\frac{p-3}{2} + 1 = \frac{p-1}{2}$ is the total number of pairs and singletons in the base case. Once position for the pair is chosen, the positions for the singletons will be determined as a result. Therefore we have the binomial expression $\binom{\frac{p-1}{2}}{1}$. This is exactly the case when $i = 0$, i.e., 1 pair.

Now we must examine what happens when the number of pairs increases. We know that the number of pairs must always be odd, so we will always increase by 2 pairs. If the number of pairs goes up, then the number of singletons must go down. It is easy to see that $b, b+1, b+3, b+4$ (2 pairs) and $b, b+2, b+4$ (3 singletons) generate exactly the same elements of R, namely $b, b+1, b+2, b+3, b+4, b+5$ so going up by 2 pairs will decrease the number of singletons by 3. This can only be done if the number of singletons is 3 or greater.

Recall that the number of singletons starts at $\frac{p-3}{2}$.

Using this information we have an inequality that we can rewrite as follows.

$\frac{p-3}{2} - 3i \geq 0 \Rightarrow 3i \leq \frac{p-3}{2} \Rightarrow 6i \leq p-3 \Rightarrow 6i+3 \leq p \Rightarrow 2i+1 \leq \frac{p}{3} < \lceil \frac{p}{3} \rceil$.

So we see that that this condition on the total number of singletons gives us an upper bound on our number of pairs. We can also solve this inequality for i to more elegantly express the limit that we will sum over:

$\frac{p-3}{2} - 3i \geq 0 \Rightarrow 3i \leq \frac{p-3}{2} \Rightarrow i \leq \frac{p-3}{6} < \lceil \frac{p-3}{6} \rceil$.

In essence, i represents the number of times the original number of singletons can go down by a multiple of 3. The number of pairs as a result of this is always

represented by $2i+1$, as every time singletons go down by 3, pairs go up by 2.

Cardinality wise, increasing by 2 pairs and decreasing by 3 singletons leads to an increase of cardinality by 1 which is exactly how the cardinality must increase. Therefore we know that any number of pairs and singletons is represented by $\frac{p-3}{2} - 3i$ (singletons) and $2i+1$ (pairs) with the condition that i starts at 0 and increases by 1 so long as $2i+1 < \lceil \frac{p}{3} \rceil$ or $i < \lceil \frac{p-3}{6} \rceil$.

Therefore the number of pairs and singletons is equal to

$\frac{p-3}{2} - 3i + 2i + 1 = \frac{p-3}{2} - i + 1 = \frac{p-1}{2} - i$.

Since there must always be at least 1 pair and the total number of pairs are odd we see that this is precisely the expression $2i+1$. As before, once the places for the pairs are chosen from the possible positions the remaining positions must be assigned to singletons.

Therefore $d = \sum_{i=0}^{i<\lceil \frac{p-3}{6} \rceil} \binom{\frac{p-1}{2}-i}{2i+1}$. □

Example 3.4 $Z/(11)$

$\lceil \frac{11-3}{6} \rceil = 2$.

$d = \sum_{i=0}^{i<2} \binom{\frac{11-1}{2}-i}{2i+1} = \binom{\frac{11-1}{2}-0}{2(0)+1} + \binom{\frac{11-1}{2}-1}{2(1)+1} = \binom{5}{1} + \binom{4}{3} = 5 + 4 = 9$

Example 3.5 $Z/(13)$

$\lceil \frac{13-3}{6} \rceil = 2$.

$d = \sum_{i=0}^{i<2} \binom{\frac{13-1}{2}-i}{2i+1} = \binom{\frac{13-1}{2}-0}{2(0)+1} + \binom{\frac{13-1}{2}-1}{2(1)+1} = \binom{6}{1} + \binom{5}{3} = 6 + 10 = 16$

Example 3.6 $Z/(17)$

$\lceil \frac{17-3}{6} \rceil = 3$.

$d = \sum_{i=0}^{i<3} \binom{\frac{17-1}{2}-i}{2i+1} = \binom{\frac{17-1}{2}-0}{2(0)+1} + \binom{\frac{17-1}{2}-1}{2(1)+1} + \binom{\frac{17-1}{2}-2}{2(2)+1} = \binom{8}{1} + \binom{7}{3} + \binom{6}{5} = 8 + 35 + 6 = 49$

Example 3.7 $Z/(19)$

$\lceil \frac{19-3}{6} \rceil = 3.$

$d = \sum_{i=0}^{i<3} \binom{\frac{19-1}{2}-i}{2i+1} = \binom{\frac{19-1}{2}-0}{2(0)+1} + \binom{\frac{19-1}{2}-1}{2(1)+1} + \binom{\frac{19-1}{2}-2}{2(2)+1} = \binom{9}{1} + \binom{8}{3} + \binom{7}{5} = 9 + 56 + 21 = 86$

We now wish to move to a slightly more general case.

Theorem 3.8 Let $R = Z/(p^n)$ where p is an odd prime. Let $E = \{0, 1\}$. Define $m = p^{n-1}$. Let d be the number of possible minimal sets of units with respect to E. Then $d = \sum_{i_j=0}^{i_j<\lceil \frac{p-3}{6} \rceil} \binom{\frac{p-1}{2}-i_1}{2i_1+1}\binom{\frac{p-1}{2}-i_2}{2i_2+1}\cdots\binom{\frac{p-1}{2}-i_m}{2i_m+1}$.

Note: this sum is over all possible combinations of i's.

Proof. We have already proved this for $n = 1$.

Let B_p be the collection of optimal sets for $Z/(p)$.

There are m copies of $Z/(p)$ in R. In each copy, it turns out it is exactly the case for $n = 1$, just with a multiple of p added to each unit in that optimal set. This is because we know from properties of the Jacobson radical that a unit plus an element in the radical is still a unit. A collection of optimal sets for one of the m copies looks like $sp + B_p$ for one $s \in \{0, 1, \cdots m - 1\}$.

Therefore the cardinality of the larger set of units depends on the cardinality of each of the m copies/subsets but each of those m copies varies in exactly the same way as sets did for $Z/(p)$, the case when $s = 0$. Now s varies independently but the cardinality of B_p remains constant in each of the m copies which is why the sum must happen over all possible i_j which only depends on p. It should be clear that an optimal set requires all m copies to be optimal.

So the first sum is always the optimal set with each $i_j = 0$. An increase in

cardinality by one in the minimal set means that exactly one of the m copies of $Z/(p)$ must increase by one. This is why to account for all the different increases of cardinality from the optimal set to the biggest minimal set we must account for all the different permutations of the i_j. If r is the largest that i_j can be, then there will be $(r+1)^m$ sums. □

We now generalize this result even further.

Theorem 3.9

Let F be a finite field of order p^n and let $m = p^{n-1}$. Let $E = \{0, 1\}$.

Let d be the number of possible minimal sets of units with respect to E.

Then $d = \sum_{i_j=0}^{i_j<\lceil \frac{p-3}{6} \rceil} \binom{\frac{p-1}{2}-i_1}{2i_1+1}\left(2\binom{\frac{p-1}{2}-i_2}{2i_2+1} + 2\binom{\frac{p-1}{2}-i_2-1}{2i_2}\right)\cdots\left(2\binom{\frac{p-1}{2}-i_m}{2i_m+1} + 2\binom{\frac{p-1}{2}-i_m-1}{2i_2}\right)$

Note: this sum is over all possible combinations of i's.

Proof. We have already proved this for $n = 1$.

For $n > 1$ what changes is that we have more units. More units means more possible minimal sets. However, we know that minimal sets picked in the way we did before will still work; so we start there. Since our idempotents are 0 and 1 we are limited in how many new minimal sets we can obtain. Before we started with 1 and ended with $p-1$ since p was not a unit. For $n \geq 1$ there exists $a \in F$, $a \notin Z/(p)$ which means a is a non trivial unit. Therefore not only would sets from $a+1$ to $a+p-1$ work as before, the sets from $a+0$ to $a+p-2$ would also work. These are new and distinct sets as the first contains $a+p-1$ but never a and the second contains a but never $a+p-1$. Therefore for $n > 1$ we already will have double the number of minimal sets compared to before.

However, this is not the only change that can occur. We can't do another shift since that would be identical to the original minimal sets. What we can do is change where we start and end so that is is different than both of the minimal sets we already have. That is to say we start at $a+0$ and end at $a+p-1$. Sets of this form are distinct from the previous since $a+0$ and $a+p-1$ are always in both but this is not possible for the previous two kinds of minimal sets. The construction of these sets is very similar to the construction of the minimal sets from before and it is still true that there must always be an odd number of pairs.

However, due to the cyclic nature, we have in fact already chosen a pair, $a+p-1, a+p-1+1 = a+0$. Therefore we have one less pair to choose so we decrease from choosing $2i+1$ pairs to $2i$. The number of singletons in the base case is still the same, namely $\frac{p-3}{2}$ singletons. Note $\frac{p-1}{2}-1 = \frac{p-3}{2}$ which is why in the new base case we have $\frac{p-1}{2}-1$ since for $i=0$ the pair has already been chosen so all that is left is for the singletons to be chosen. As i increase we still keep in mind that the pairs must be odd but that we have already chosen one, so that is why we will choose $2i$ pairs in the general case. As before, an increase in i leads to a decrease of the number of the total number of singletons and pairs as we saw before thus our general case of $\frac{p-1}{2-i}$. Now that we have this case we can also see that shifting by one will also produce another identical minimal set, going from $a+1$ to $a+p-1+1 = a+p = a$ will be distinct from all previous cases. To summarize:

Case 1. From $a+1$ to $a+p-1$. Does not contain a so can't be case 2, 3 or 4.

Case 2. From $a+0$ to $a+p-2$. Does not contain $a+p-1$ so can't be case 1 or 3

and does not contain $a+1$ so can't be case 4.

Case 3. From $a+0$ to $a+p-1$. Does not contain $a+1$ so can't be case 1 or 4 and does not contain $a+p-2$ so can't be case 2.

Case 4. From $a+1$ to a. Does not contain $a+p-1$ so can't be case 1 or 3 and contains $a+1$ so can't be case 2.

Therefore $d = \sum_{i_j=0}^{i_j<\lceil \frac{p-3}{6} \rceil} \binom{\frac{p-1}{2}-i_1}{2i_1+1}\left(2\binom{\frac{p-1}{2}-i_2}{2i_2+1}+2\binom{\frac{p-1}{2}-i_2-1}{2i_2}\right)\cdots\left(2\binom{\frac{p-1}{2}-i_m}{2i_m+1}+2\binom{\frac{p-1}{2}-i_m-1}{2i_2}\right)$

□

We now generalize the most that we can at this time.

Conjecture 3.10

Let R be a finite commutative ring. Let $E=\{0,1\}$. Then $R \cong L_1 \times L_2 \times \cdots \times L_t$ where t is finite and each L_h is a local ring. The set of idempotents for R is $(a_1, a_2, \cdots, a_t)$ where each a_h is 0 or 1. Let M_h be the maximal ideal of L_h. Let $F_h = \frac{L_h}{M_h}$ be the finite field associated with each local ring. $\mid F_h \mid = p_h^{n_h} = f_h$ and the composition length of L_h is t_h and $m_h = p_h^{n_h-1}$.

The number of total possible minimal sets for each local ring L_h is d_h with

$$d_h = \sum_{i_{j_k}=0}^{i_{j_k}<\lceil \frac{p-3}{6} \rceil}$$

$$\left[\binom{\frac{p-1}{2}-i_{1_1}}{2i_{1_1}+1}\left(2\binom{\frac{p-1}{2}-i_{2_1}}{2i_{2_1}+1}+2\binom{\frac{p-1}{2}-i_{2_1}-1}{2i_{2_1}}\right)\cdots\left(2\binom{\frac{p-1}{2}-i_{m_1}}{2i_{m_1}+1}+2\binom{\frac{p-1}{2}-i_{m_1}-1}{2i_{m_1}}\right)\right]$$

$$\left[\binom{\frac{p-1}{2}-i_{1_2}}{2i_{1_2}+1}\left(2\binom{\frac{p-1}{2}-i_{2_2}}{2i_{2_2}+1}+2\binom{\frac{p-1}{2}-i_{2_2}-1}{2i_{2_2}}\right)\cdots\left(2\binom{\frac{p-1}{2}-i_{m_2}}{2i_{m_2}+1}+2\binom{\frac{p-1}{2}-i_{m_2}-1}{2i_{m_2}}\right)\right]$$

$$\left[\binom{\frac{p-1}{2}-i_{1_{t_h}}}{2i_{1_{t_h}}+1}\left(2\binom{\frac{p-1}{2}-i_{2_{t_h}}}{2i_{2_{t_h}}+1}+2\binom{\frac{p-1}{2}-i_{2_{t_h}}-1}{2i_{2_{t_h}}}\right)\cdots\left(2\binom{\frac{p-1}{2}-i_{m_{t_h}}}{2i_{m_{t_h}}+1}+2\binom{\frac{p-1}{2}-i_{m_{t_h}}-1}{2i_{m_{t_h}}}\right)\right]$$

So for R the number of total possible minimal sets of units D is

$D = d_1 \times d_2 \times \cdots \times d_t$ Note: this sum is over all possible combinations of i_{j_k}'s

with $j \in \{1, 2, 3, \cdots p^{n-1}\}$, $k \in \{1, 2, 3, \cdots t_h\}$

Since we only state this as a conjecture we now give some intuition for the result.

We know this is true when the composition length is 1 as we just have a finite field. However, when we have nontrivial composition length, this is just a certain numbers of copies of our finite field for our purposes. These copies must all be allowed to vary in cardinality independently if we are to get all the possibilities over the entire local ring. But this is precisely the same thing that happens when going from $Z/(p)$ to $Z/(p^n)$ in our earlier work.

$$d_h = \sum_{i_{j_k}=0}^{i_{j_k} < \lceil \frac{p-3}{6} \rceil}$$

$$[\tbinom{\frac{p-1}{2}-i_{1_1}}{2i_{1_1}+1}(2\tbinom{\frac{p-1}{2}-i_{2_1}}{2i_{2_1}+1} + 2\tbinom{\frac{p-1}{2}-i_{2_1}-1}{2i_{2_1}}) \cdots (2\tbinom{\frac{p-1}{2}-i_{m_1}}{2i_{m_1}+1} + 2\tbinom{\frac{p-1}{2}-i_{m_1}-1}{2i_{m_1}})]$$

$$[\tbinom{\frac{p-1}{2}-i_{1_2}}{2i_{1_2}+1}(2\tbinom{\frac{p-1}{2}-i_{2_2}}{2i_{2_2}+1} + 2\tbinom{\frac{p-1}{2}-i_{2_2}-1}{2i_{2_2}}) \cdots (2\tbinom{\frac{p-1}{2}-i_{m_2}}{2i_{m_2}+1} + 2\tbinom{\frac{p-1}{2}-i_{m_2}-1}{2i_{m_2}})]$$

$$[\tbinom{\frac{p-1}{2}-i_{1_{t_h}}}{2i_{1_{t_h}}+1}(2\tbinom{\frac{p-1}{2}-i_{2_{t_h}}}{2i_{2_{t_h}}+1} + 2\tbinom{\frac{p-1}{2}-i_{2_{t_h}}-1}{2i_{2_{t_h}}}) \cdots (2\tbinom{\frac{p-1}{2}-i_{m_{t_h}}}{2i_{m_{t_h}}+1} + 2\tbinom{\frac{p-1}{2}-i_{m_{t_h}}-1}{2i_{m_{t_h}}})]$$

The result of this is that for any finite commutative ring R, the number of total possible minimal sets of units D is

$D = d_1 \times d_2 \times \cdots \times d_t$

This concludes the intuition for the result.

CHAPTER 4
EXAMPLES FOR 2 BY 2 MATRICES

In clean rings an element is by definition the sum of an idempotent and a unit. In some instances an element can be expressed in multiple ways. For example $x = e_1 + u_1$ and $x = e_2 + u_2$ with $e_1 \neq e_2$, $u_1 \neq u_2$. Throughout the course of our work we focus on $\{0, 1\}$ diagonal idempotents and that will continue here. We find that some elements may be uniquely expressed with respect to the $\{0, 1\}$ diagonal idempotents. That is to say that the element is the sum of one specific $\{0, 1\}$ diagonal idempotent and one specific unit. For the purposes of our work we will call an element that is uniquely expressed in this way diagonal idempotent unique to emphasize this property.

Definition 4.1 A is *diagonal idempotent unique* if there exists only one specific unit U and $\{0, 1\}$ diagonal idempotent E whose sum is A.

Theorem 4.2: A matrix element

$$A = \begin{bmatrix} a & b \\ \\ c & d \end{bmatrix}$$

with entries from any ring R with $char(R) \neq 2$ is diagonal idempotent unique if and only if the diagonal entries a and d are 0 or 1 and $bc = 0$.

Consequently, if A is diagonal idempotent unique with respect to an idempotent E this means that for all $F \neq E$ that $det(A - F) = 0$.

Conversely, if for all diagonal idempotents except for one, $det(A - F) = 0$, then A is diagonal idempotent unique.

Proof. We first will prove the left to right direction.

Let $E_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, $E_3 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $E_4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Case 1. A is diagonal idempotent unique with idempotent E_1

Therefore $det(A - E_1) = ad - bc \neq 0$ (1).

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 0$ (2).

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 0$ (3).

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 0$ (4).

Using (2) in (4) yields $-d + 1 = 0$ or $d = 1$.

Using (3) in (4) yields $-a + 1 = 0$ or $a = 1$.

Using $a = 1$ and $d = 1$ in (4) yields $bc = 0$.

Using $a = 1$, $d = 1$ and $bc = 0$ in all 4 equations checks out.

Therefore we have proved Case 1.

Case 2. A is diagonal idempotent unique with idempotent E_2.

Therefore $det(A - E_1) = ad - bc = 0$ (1).

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc \neq 0$ (2).

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 0$ (3).

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 0$ (4).

Using (1) in (3) yields $-d = 0$ or $d = 0$.

Using (1) and $d = 0$ in (4) yields $-a + 1 = 0$ or $a = 1$.

Using $a = 1$ and $d = 0$ in (1) yields $-bc = 0$ or $bc = 0$.

Using $a = 1$, $d = 0$ and $bc = 0$ in all 4 equations checks out.

Therefore we have proved Case 2.

Case 3. A is diagonal idempotent unique with idempotent E_3.

Therefore $det(A - E_1) = ad - bc = 0$ (1).

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 0$ (2).

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc \neq 0$ (3).

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 0$ (4).

Using (1) in (2) yields $-a = 0$ or $a = 0$.

Using (1) and $a = 0$ in (4) yields $-d + 1 = 0$ or $d = 1$.

Using $a = 0$ and $d = 1$ in (1) yields $-bc = 0$ or $bc = 0$.

Using $a = 0$, $d = 1$ and $bc = 0$ in all 4 equations checks out.

Therefore we have proved Case 3.

Case 4. A is diagonal idempotent unique with idempotent E_4.

Therefore $det(A - E_1) = ad - bc = 0$ (1).

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 0$ (2).

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 0$ (3).

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc \neq 0$ (4).

Using (1) in (2) yields $-a = 0$ or $a = 0$.

Using (1) in (3) yields $-d = 0$ or $d = 0$.

Using $a = d = 0$ in (1) yields $-bc = 0$ or $bc = 0$.

Using $a = d = 0$ and $bc = 0$ in all 4 equations checks out.

Therefore we have proved Case 4.

Therefore we have proved this in the left to right direction.

Now we will prove this in the right to left direction.

Case 1. $a = d = 0$ and $bc = 0$.

Therefore $det(A - E_1) = ad - bc = 0 - 0 = 0$.

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 0 - 0 - 0 = 0$.

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 0 - 0 - 0 = 0$.

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 0 - 0 - 0 + 1 - 0 = 1 \neq 0$.

So the matrix is diagonal idempotent unique and it is unique for the diagonal idempotent $E_4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Case 2. $a = 0$,$d = 1$ and $bc = 0$.

Therefore $det(A - E_1) = ad - bc = 0 - 0 = 0$.

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 0 - 0 - 0 = 0$.

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 0 - 1 - 0 \neq 0$.

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 0 - 0 - 1 + 1 - 0 = 0$.

So the matrix is diagonal idempotent unique and it is unique for the diagonal idempotent $E_3 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

Case 3. $a = 1$,$d = 0$ and $bc = 0$.

Therefore $det(A - E_1) = ad - bc = 0 - 0 = 0$.

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 0 - 1 - 0 = -1 \neq 0$.

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 0 - 0 - 0 = 0$.

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 0 - 1 - 0 + 1 - 0 = 0$.

So the matrix is diagonal idempotent unique and it is unique for the diagonal idem-

potent $E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

Case 4. $a = d = 1$ and $bc = 0$.

Therefore $det(A - E_1) = ad - bc = 1 - 0 = 1 \neq 0$.

Therefore $det(A - E_2) = a(d-1) - bc = ad - a - bc = 1 - 1 - 0 = 0$.

Therefore $det(A - E_3) = (a-1)d - bc = ad - d - bc = 1 - 1 - 0 = 0$.

Therefore $det(A - E_4) = (a-1)(d-1) - bc = ad - a - d + 1 - bc = 1 - 1 - 1 + 1 - 0 = 0$.

So the matrix is diagonal idempotent unique and it is unique for the diagonal idempotent $E_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Therefore we have proved this in the right to left direction. □

4.1 Diagonal Idempotent Unique Decompositions for $M_2(Z/(p))$

We now explicitly compute the diagonal idempotent unique decompositions for $M_2(Z/(p))$ for a prime p. Note that 1 and $p-1$ are always units in $Z/(p)$.

When $p \neq 2$ we will have the following unique elements and their respective diagonal idempotents and units for $M_2(Z/(p))$. Note $bc = 0$ in all types.

Type 1

$$\begin{bmatrix} 0 & b \\ c & 1 \end{bmatrix} = \begin{bmatrix} p-1 & b \\ c & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Type 2

$$\begin{bmatrix} 1 & b \\ c & 0 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & p-1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Type 3

$$\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} = \begin{bmatrix} p-1 & b \\ c & p-1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Type 4

$$\begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

We can see from the Type 4 case that the identity element is always diagonal idempotent unique, i.e, when $b = c = 0$ in Type 4.

For each type there are $(p-1)(1) + (1)(p-1) + (1)(1) = 2p-1$ possible ways for $bc = 0$. Therefore in general there are $4(2p-1) = 8p-4$ diagonal idempotent unique elements for $M_2(Z/(p))$ for $p \neq 2$.

Note $p = 2$ is a special case since $p - 1 = 1$ and also very nice as we shall see.

4.2 Optimal sets for $M_2(Z/(2))$

Now we will compute an optimal set of units over $R = M_2(Z/(2))$ with the diagonal idempotents

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

We will look at the additive cosets of R according to the choices of b and c in $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Note there are 4 diagonal idempotents and 4 cosets as well as $2^4 = 16$ total elements in $M_2(Z/(2))$. Also note that in each coset only the diagonal entries a and d can be changed by the diagonal idempotents.

Coset 1. $b = c = 0$. Only 1 unit to choose.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Adding this unit with the 4 diagonal idempotents yields all elements of this coset.

Coset 2. $b = 1$ and $c = 0$. Only 1 unit to choose.

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Adding this unit with the 4 diagonal idempotents yields all elements of this coset.

Coset 3. $b = 0$ and $c = 1$. Only 1 unit to choose.

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Adding this unit with the 4 diagonal idempotents yields all elements of this coset.

Coset 4. $b = c = 1$. 3 units to choose. Any will work. Without loss of generality we choose $a = d = 0$.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Adding this unit with the 4 diagonal idempotents yields all elements of this coset.

So we know that an optimal set of units for $M_2(Z/(2))$ has 4 units, 3 possible choices

and one such choice of units is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

.

4.3 Optimal sets for $M_2(Z/(3))$

Now consider $M_2(Z/(3))$. We will now compute the special case for the cardinality of an optimal set for $M_2(Z/(3))$ using our previous work of diagonal idempotent unique elements and brute force calculations. Now $p = 3$ is the first odd prime and exhibits more of the general behavior we would expect from an arbitrary prime so it is useful to understand this case and with 81 elements this matrix ring is not trivial. In general, finding the cardinality of an optimal set of units seems difficult. As p gets larger it becomes more complicated to calculate solutions and there seem to be strong ties to graph theory type problems.

From our previous work we know that b and c play a pivotal role in the diagonal idempotent unique elements. With this in mind we will break up $M_2(Z/(3))$ into additive cosets like before where b and c are fixed. So in this case each coset will have 9 (p choices for a, p choices for d) elements and there will be 9 (p choices for b, p choices for c) cosets.

We begin by examining the cosets where $bc = 0$ since these give rise to the diagonal idempotent unique elements and any optimal minimal set must contain the units corresponding to these diagonal idempotent unique elements. There are 5 $(2p - 1)$ cosets where $bc = 0$. $b = c = 0$, $b = 1$ and $c = 0$, $b = 2$ and $c = 0$, $b = 0$ and $c = 1$

and $b = 0$ and $c = 2$.

From above we know there are 4 types so there are 4 required units in each of these cosets. Since $bc = 0$ the other 5 elements in these cosets are not units and not possible choices, but these 4 units in each coset are enough to span the coset as we will show now.

Consider the following generic units for $bc = 0$

$$\begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix}, \begin{bmatrix} 2 & b \\ c & 2 \end{bmatrix}, \begin{bmatrix} 1 & b \\ c & 2 \end{bmatrix} \text{ and } \begin{bmatrix} 2 & b \\ c & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} = \begin{bmatrix} 2 & b \\ c & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & b \\ c & 0 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & b \\ c & 0 \end{bmatrix} = \begin{bmatrix} 2 & b \\ c & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & b \\ c & 1 \end{bmatrix} = \begin{bmatrix} 2 & b \\ c & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & b \\ c & 1 \end{bmatrix} = \begin{bmatrix} 2 & b \\ c & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & b \\ c & 2 \end{bmatrix} = \begin{bmatrix} 2 & b \\ c & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & b \\ c & 2 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & b \\ c & 2 \end{bmatrix} = \begin{bmatrix} 2 & b \\ c & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

So we have shown that each of these 5 cosets require 4 units each so an optimal set of units must contain these 20 units.

Now consider the 4 cosets where $bc \neq 0$. In each of these types of cosets there are 5 units so at worst we might have to choose all 5. At best we have to choose more than 2 so a minimum of 3. We will show that exactly 3 can be chosen from each coset by giving explicit examples, though more than one choice may be possible.

Coset 1. $b = c = 1$. A possible choice of units is

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Coset 2. $b = c = 2$. A possible choice of units is

$$\begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Coset 3. $b = 1$ and $c = 2$. A possible choice of units is

$$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Coset 4. $b = 2$ and $c = 1$. A possible choice of units is

$$\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

So we know that an optimal set for each of these 4 cosets has exactly 3 units each, which adds 12 more units to the set. Therefore an optimal set of units for $Mat_2(Z/(3))$ with respect to the $\{0, 1\}$ diagonal idempotents contains exactly 32 units with a possible set of units given above for each coset.

CHAPTER 5
UNIQUE ELEMENTS FOR N BY N MATRICES

We begin by abstracting the determinant property of upper (respectively lower) triangular matrices. It is known that if a matrix T is upper (respectively lower) triangular that the determinant of T is easily computable. That is, $det(T) = a_{1,1} \times a_{2,2} \times \cdots \times a_{n-1,n-1} \times a_{n,n}$. One of the methods for determining if a matrix element is diagonal idempotent unique involves subtracting all of the possible $\{0, 1\}$ diagonal idempotents from an element and then taking the determinant of these new matrices. If all except for one yield zero, then the matrix element was diagonal idempotent unique. Since subtracting $\{0, 1\}$ diagonal idempotents only changes the diagonal entries of the original matrix element and since taking determinants in general can be cumbersome, it would be nice to only have to compute the product of the diagonals to compute the determinant. However, rather than restrict ourselves to the cases of upper and lower triangular matrices we abstract the property of these kinds of matrices to allow us to deal with a more general property which we have named quasi-uppper (or lower) triangular.

Let F be a field.

Definition 5.1 $A \in M_n(F)$ is said to be *quasi-upper triangular* if there is exactly 1 row and column with 0 off-diagonal zeros, 1 row and column with 1 off-diagonal zeros, 1 row and column with 2 off-diagonal zeros, ... and 1 row and column with $n - 1$ off-diagonal zeros.

Theorem 5.2 Let $A \in M_n(F)$ with the following properties.

1) A is quasi-upper triangular

2) The diagonal entries $a_{i,i}$ must be 0 or 1.(This is related to the idempotent it is diagonal idempotent unique for)

3) $a_{i,j}a_{j,i} = 0$ for every i, j with $i \neq j$.

Then the matrix element $A \in M_n(F)$ is diagonal idempotent unique.

Proof. Recall A is diagonal idempotent unique if there exist only one specific unit U and diagonal idempotent E that add together to create A. This means that for all diagonal $F \neq E$, that $det(A - F) = 0$. Conversely, if for all idempotents except for one, $det(A - F) = 0$, then A is unique.

Assume the diagonal entries $a_{i,i}$ are 0 or 1 and $a_{i,j}a_{j,i} = 0$ for every i, j with $i \neq j$. and there is exactly 1 row and column with 0 off-diagonal zeros, 1 row and column with 1 off-diagonal zeros, 1 row and column with 2 off-diagonal zeros, ... and 1 row and column with $n - 1$ off-diagonal zeros.

We will have all diagonal entries be 0 for the purposes of our calculations. We will see later that when we subtract any other idempotent except $E = I$ that there will be a zero on the diagonal which will give us a determinant of 0 as desired. All one has to do for the other $2^n - 1$ possible matrices is run the same argument and notice that $a_{i,i} + e_{i,i} = 1$ where $e_{i,i}$ is the corresponding diagonal entry in the idempotent matrix E that is the idempotent that A is diagonal idempotent unique with respect to. For all other idempotents, $a_{i,i} - e_{i,i} = 0$ at least once.

Let $\sigma \in S_n$ be a permutation such that the $\sigma(1)$ row represents the row with $n-1$ off-diagonal zeros, the $\sigma(2)$ row represents the row with $n-2$ off-diagonal zeros,

... the $\sigma(n)$ row represents the row with 0 off-diagonal zeros. Due to the transpose condition $a_{i,j}a_{j,i} = 0 \; \forall i \neq j$ we know that the $\sigma(1)$ column has 0 off-diagonal zeros, ... the $\sigma(n)$ column has $n-1$ zeros.

We now take the determinant of A by cofactor expansion. We can take the determinant along any row or column at any step though there is only 1 row or column we will possibly choose at each step. With 2 choices at each step, there will be 2^n possible determinants but all with the same result. We will show the determinant that is obtained by choosing a row at every step.

First we will take the determinant along the $\sigma(1)$ row. Since the $\sigma(1)$ row has $n-1$ off-diagonal zeros, $det(A) = (-1)^{\sigma(1)+\sigma(1)} a_{\sigma(1),\sigma(1)} * det(A_1) = a_{\sigma(1),\sigma(1)} * det(A_1)$ where A_1 is the matrix obtained by removing the $\sigma(1)$ row and $\sigma(1)$ column. Due to the property of the original matrix A we know that there are no off-diagonal zeros in the $\sigma(1)$ column so the $n-1$ rows of A_1 still have the same number of zeros. Also, due to $\sigma(1)$ row having $n-1$ off-diagonal zeros we know that the remaining columns in A_1 each lose exactly 1 zero meaning that A_1 satisfies exactly the same properties as A just one dimension smaller.

Now we will take the determinant along the $\sigma(2)$ row. Since the $\sigma(2)$ row has $n-2$ off-diagonal zeros, $det(A) = a_{\sigma(1),\sigma(1)} * a_{\sigma(2),\sigma(2)} * det(A_2)$ where A_2 is the matrix obtained by removing the $\sigma(1)$ and $\sigma(2)$ rows and $\sigma(1)$ and $\sigma(2)$ columns from A. Similarly, A_2 satisfies the same properties as A just two dimensions smaller.

We proceed in the exact same fashion until we get to A_{n-2} which is a 2 by 2 matrix with the same properties as A just $n-2$ dimensions smaller. Now $det(A_{n-2}) =$

$a_{\sigma(n-1),\sigma(n-1)} * a_{\sigma(n),\sigma(n)} - a_{\sigma(n-1),\sigma(n)} * a_{\sigma(n),\sigma(n-1)} = a_{\sigma(n-1),\sigma(n-1)} * a_{\sigma(n),\sigma(n)}$ since $a_{\sigma(n-1),\sigma(n)} = 0$.

So we know $det(A) = a_{\sigma(1),\sigma(1)} * a_{\sigma(2),\sigma(2)} * \cdots * a_{\sigma(n-1),\sigma(n-1)} * a_{\sigma(n),\sigma(n)}$ which is simply the product of the diagonal entries. As mentioned above if A has the row and column property assumed we call this quasi-upper (or lower) triangular as the determinant is just the product of the diagonals.

Now we examine the possibilities of subtracting every possible idempotent from A. Subtracting idempotents only effects diagonal entries so the off diagonal property of being quasi-upper triangular is preserved which means the determinant of the resulting matrix is also just the product of the diagonals.

Since the diagonal entries are all 0, this means that the only idempotent that will change every diagonal entry to a non-zero entry in the matrix $A-E$ (namely -1) is the identity idempotent so $det(A-I) = (-1)^n \neq 0$. For all $F \neq I$ the determinant of $A-F$ will be zero since at least one diagonal entry of $A-F$ will be 0. This is the requirement for A to be diagonal idempotent unique. □

We suspect and believe that this proof is actually if and only if. However, due to the difficulty of computing 2^n determinants with entries unknown and then using those determinants in a series of substitutions that gets increasingly more difficult as n increases we are only able to prove the one direction at this time. We believe that with more work in the future and possibly with collaboration that this can become an if and only if proof. This would be significant because we would know that diagonal idempotent unique elements would only have a very specific form and any element

not of that form could not be diagonal idempotent unique. However, this result gives us a lower bound on the number of diagonal idempotent unique elements in $M_n(F)$ and is suggestive of the fact that only the diagonal entries are important in the determinant of diagonal idempotent unique entries and as a result all other paths in the determinant must be 0 for all idempotents.

CHAPTER 6
ROW REDUCED MATRICES

Row reduced matrices are a very important class of elements in linear algebra and other areas of mathematics. It therefore seems natural to ask which matrices can be represented as a sum of an invertible matrix and a row reduced matrix. As with previous work, we will discuss some special cases.

Consider a 2 by 2 matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over a finite field F. We ask, when can we find a row reduced matrix R with $M - R$ invertible?

Let us start with $R = \begin{bmatrix} 1 & x_0 \\ 0 & 0 \end{bmatrix}$

Suppose for every x_0 we have $det(M - R) = det\left(\begin{bmatrix} a-1 & b-x_0 \\ c & d \end{bmatrix}\right) \neq 0$

Then we want $(a-1)d - c(b-x_0) \neq 0$.

Theorem 6.1: Let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $R = \begin{bmatrix} 1 & x_0 \\ 0 & 0 \end{bmatrix}$ with entries from a finite field F.

1) If $c = 0$, then M is a sum of an invertible matrix and a row reduced matrix R $\iff a \neq 1, d \neq 0$.

2) If $a = 1$ or $d = 0$, then M is a sum of an invertible matrix and a row reduced matrix $R \iff b \neq x_0, c \neq 0$.

3) If $a = 1$ and $c = 0$ or $d = 0$ and $c = 0$ then M is not a sum of an invertible matrix and a row reduced matrix R, i.e., M is already row reduced.

Proof. $det(M-R) = (a-1)d - c(b-x_0)$.

Case 1. $c = 0$. Then $det(M-R) = (a-1)d - c(b-x_0) = (a-1)d \neq 0 \iff a \neq 1, d \neq 0$

Case 2. $a = 1$ or $d = 0$. Then $det(M-R) = (a-1)d - c(b-x_0) = -c(b-x_0) \neq 0 \iff b \neq x_0, c \neq 0$

Case 3. $a = 1$ and $c = 0$ or $d = 0$ and $c = 0$. Then $det(M-R) = (a-1)d - c(b-x_0) = 0 \implies M-R$ is not invertible. □

Thus we already see that for 2 by 2 matrices it is not possible for every element to be the sum of a row reduced matrix and an invertible matrix.

Now we move on to discuss the 3 by 3 case.

Let $A = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$

To facilitate computation we assume $a_{1,1} \neq 1$

We want to subtract a 3 by 3 row reduced matrix R and get $det(A-R) \neq 0$.

We start with $R_1 = \begin{bmatrix} 1 & x & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ and then suppose that for every x and y

$$det(A-R_1) = det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,2}-x & a_{1,3}-y \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}\right) = 0$$

Then we have:

$$(a_{1,1}-1)det\left(\begin{bmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{bmatrix}\right) - (a_{1,2}-x)det\left(\begin{bmatrix} a_{2,1} & a_{2,3} \\ a_{3,1} & a_{3,3} \end{bmatrix}\right)$$

$$+(a_{1,3}-y)det\left(\left[\begin{array}{cc} a_{2,1} & a_{2,2} \\ a_{3,1} & a_{3,2} \end{array}\right]\right)=0.$$

By varying x and y and by our assumption that $a_{1,1} \neq 1$ we see that each of the sub determinants is zero. This means that the last two rows are linearly dependent.

So for this case we know that elements with the property that the 2nd and 3rd rows are linearly dependent cannot be expressed as the sum of an invertible matrix and an R_1. In addition we know that if the 2nd and 3rd rows are linearly independent then there will exist x and y so not only will at least one of the subdeterminants be nonzero but their sum will also be nonzero.

Now Let $R_2 = \left[\begin{array}{ccc} 1 & 0 & u \\ 0 & 1 & v \\ 0 & 0 & 0 \end{array}\right]$

Now we revisit our matrix A that has the 2nd and 3rd rows that are linearly dependent and we now compute

$$det\left(\left[\begin{array}{ccc} a_{1,1}-1 & a_{1,2} & a_{1,3}-u \\ a_{2,1} & a_{2,2}-1 & a_{2,3}-v \\ ka_{2,1} & ka_{2,2} & ka_{2,3} \end{array}\right]\right)=0 \text{ where } k \neq 0.$$

Then we have:

$$det\left(\left[\begin{array}{ccc} a_{1,1}-1 & a_{1,2} & a_{1,3}-u \\ a_{2,1} & a_{2,2}-1 & a_{2,3}-v \\ ka_{2,1} & ka_{2,2} & ka_{2,3} \end{array}\right]\right)=$$

$$(a_{1,1}-1)det\left(\left[\begin{array}{cc} a_{2,2}-1 & a_{2,3}-v \\ ka_{2,2} & ka_{2,3} \end{array}\right]\right)-a_{1,2}det\left(\left[\begin{array}{cc} a_{2,1} & a_{2,3}-v \\ ka_{2,1} & ka_{2,3} \end{array}\right]\right)$$

$$+(a_{1,3}-u)det\left(\begin{bmatrix} a_{2,1} & a_{2,2}-1 \\ ka_{2,1} & ka_{2,2} \end{bmatrix}\right)$$
$$=(a_{1,1}-1)(vka_{2,2}-ka_{2,3})-a_{1,2}(kva_{2,1})+(a_{1,3}-u)(ka_{2,1})$$

1) Let $v=0$ and $u=a_{1,3}$ to get $a_{2,3}=0$.

2) Let $v=0$ and $u=1+a_{1,3}$ to get $a_{2,1}=0$

3) $a_{2,3}=0$ and $a_{2,1}=0$ means $a_{2,2}=0$

So now let $R_3=I_3$ and the matrices that cannot be expressed as sums of row reduced matrices and invertible matrices look like

$$A=\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Then $det(A-R_3)=a_{1,1}-1\neq 0$ under our hypothesis.

Theorem 6.2 Let $A=\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}$ with $a_{1,1}\neq 1$, then there is a row reduced matrix R with $det(A-R)\neq 0$.

Proof. We went through all the cases above with R_1, R_2 and R_3. □

Now if $A=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ there is never a row reduced matrix R with $det(A-R)\neq 0$ as the first column of $A-R$ is identically zero or the last row is identically zero.

Now suppose the last row of A is zero. Then the only row reduced matrix we

are allowed to subtract is the identity R_3,

i.e. $det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2}-1 & a_{2,3} \\ 0 & 0 & -1 \end{bmatrix}\right) = (-1)det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,2} \\ a_{2,1} & a_{2,2}-1 \end{bmatrix}\right) = -t$

So we have a solution if and only if $t \neq 0$.

If the middle row of A is zero we let $R = \begin{bmatrix} 1 & 0 & u \\ 0 & 1 & v \\ 0 & 0 & 0 \end{bmatrix}$ and ask what happens if

$$det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,2} & a_{1,3}-u \\ 0 & -1 & -v \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix}\right) = 0$$

Then we have $(-1)det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,3}-u \\ a_{3,1} & a_{3,3} \end{bmatrix}\right) + (v)det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,2} \\ a_{3,1} & a_{3,2} \end{bmatrix}\right) = 0.$

Letting u and v vary separately we get each subdeterminant is zero and $a_{3,1} = 0$ which means that $(a_{1,1}-1)a_{3,3} = 0$ and $(a_{1,1}-1)a_{3,2} = 0$ which means if $a_{1,1} \neq 1$ that the last row must also be zero. But if that is the case we know that subtracting the identity R_3 will yield an invertible matrix.

Now consider if $a_{1,1} = 1$.

Let $A_1 = \begin{bmatrix} 1 & a_{1,2} & a_{1,3} \\ 0 & 0 & 0 \\ 0 & a_{3,2} & a_{3,3} \end{bmatrix}$

The row reduced matrix we must subtract in order to have any hope of having nonzero determinant must have a 1 in the $(2,2)$ position and since it is row reduced that must also mean it has a 1 in the $(1,1)$ position. However this means that $A_1 - R$ has

the first column identically zero which means the determinant will always be zero so it is not possible for A_1 to be expressed as the sum of a row reduced matrix and a invertible matrix.

So we make the following conclusions for when it is possible for a 3 by 3 matrix to be expressed as the sum of a row reduced matrix and an invertible matrix:

1) The problem is always solvable if $a_{1,1} \neq 1$.

2) If $a_{1,1} = 1$, there is at least one counterexample so it is not possible.

3) If the last row is zero we have a solution iff $det\left(\begin{bmatrix} a_{1,1}-1 & a_{1,2} \\ a_{2,1} & a_{2,2}-1 \end{bmatrix}\right) \neq 0$.

4) If the middle row is zero and the last row is zero we know we have a solution iff $a_{1,1} \neq 1$. (Sub case of 1)

5) If the middle row is zero and $a_{1,1} = 1$ we have the matrix A_1 which has no solution. (Another counterexample for 2)

Some of these results are suggestive and give rise to the following statement.

Conjecture

A matrix M cannot be expressed as the sum of an invertible matrix and a non identically zero row reduced matrix if M is a row reduced matrix with $a_{1,1} = 1$.

CHAPTER 7
UPPER TRIANGULAR MATRICES

We consider the set of upper triangular matrices and ask which matrices are sums of a unit and an upper triangular matrix.

If $R = M_n(Z/(p))$ where p is a prime then R has p^{n^2} elements M with

$$M = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,n} \end{bmatrix}$$

Of those elements, $p^{\frac{n^2+n}{2}}$ are upper triangular elements T with

$$T = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ 0 & 0 & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n,n} \end{bmatrix}$$

Now we pick a special set of units U with

$$U = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ a_{2,1} & 1 & 0 & \cdots & 0 \\ a_{3,1} & a_{3,2} & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n-1} & 1 \end{bmatrix}$$

There are $p^{\frac{n^2-n}{2}}$ units of this special form.

Note: Units of this form are referred to as unit lower triangular or lower unitriangular as well as normed lower triangular.

We claim that $R = T + U$, i.e., that every element can be written as the sum of an upper triangular matrix and an invertible matrix (unit). Not only that, this can be done so that every element can be uniquely expressed as a sum of an upper triangular and a unit of the given form.

Theorem 7.1: If $R = M_n(Z/(p))$ where p is a prime then $R = T + U$ with every element of R being uniquely expressed.

Proof. $M = T + U$

$$\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,n} \end{bmatrix} =$$

$$\begin{bmatrix} d_1 & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ 0 & d_2 & a_{2,3} & \cdots & a_{2,n} \\ 0 & 0 & d_3 & \cdots & a_{3,n} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & d_n \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ a_{2,1} & 1 & 0 & \cdots & 0 \\ a_{3,1} & a_{3,2} & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n-1} & 1 \end{bmatrix}$$

Where $d_i = a_{i,i} - 1$.

Also note that $p^{\frac{n^2+n}{2}}$ (the number of upper triangular units) times $p^{\frac{n^2-n}{2}}$ (the number of units in the unit lower triangular form) is

$p^{\frac{n^2+n}{2}} p^{\frac{n^2-n}{2}} = p^{\frac{n^2+n+n^2-n}{2}} = p^{\frac{2n^2}{2}} = p^{n^2}$ which is exactly the number of elements in R. Now suppose that $M_1 = T_1 + U_1$ and $M_1 = T_2 + U_2$. But $U_1 = U_2$ so that means $T_1 = T_2$ so M_1 is unique. But M_1 was arbitrary so every M is unique with respect to the given sets. □

Conjecture 7.2: In Theorem 7.1, $Z/(p)$ can be replaced by any field.

REFERENCES

[1] D. D. Anderson and V. P. Camillo. Commutative rings whose elements are a sum of a unit and idempotent. *Communications in Algebra, 30:7, 3327-3336*, 2002.

[2] V. P. Camillo and D. Khurana. A characterization of unit-regular rings. *Communications in Algebra, 29, 2293-2295*, 2001.

[3] V. P. Camillo and Hua-Ping Yu. Exchange rings, units, and idempotents. *Communications in Algebra, 22:12, 4737-4749*, 1994.

[4] J. Han and W. K. Nicholson. Extensions of clean rings. *Communications in Algebra, 29, 2589-2595*, 2001.

[5] D. Khurana and T. Y. Lam. Clean matrices and unit-regular matrices. *Journal of Algebra, 280, 683-698*, 2004.

[6] T. Y. Lam. *Lectures on Modules and Rings, Grad. Texts in Math., vol 189.* Springer-Verlag, New York, 1999.

[7] T. Y. Lam. *A First Course in Noncommutative Rings, second ed., Grad. Texts in Math., vol. 131.* Springer-Verlag, New York, 2001.

[8] W. K. Nicholson. Lifting idempotents and exchange rings. *Trans. Amer. Math. Soc. 229 , 269-278*, 1977.

[9] W. K. Nicholson. Strongly clean rings and fitting's lemma. *Communications in Algebra, 27:8, 3583-3592*, 1999.