Two Topics in Algebra and Number Theory

by

Makoto Suwama

(Under the Direction of Dino Lorenzini)

Abstract

Given any commutative ring R, a commutator of two $n \times n$ matrices over R has trace 0. In the first part of the dissertation, we study the converse: whether every $n \times n$ trace 0 matrix is a commutator. We show that over a Bézout domain with an algebraically closed quotient field, every trace 0 matrix is a commutator. We then show that if R is a regular ring with a large enough dimension, then there exist an $n \times n$ trace 0 matrix that is not a commutator. This improves on a result of Lissner by increasing the size of the matrix n allowed for a fixed R.

In the second part, we study cycles associated with the b-ary expansion of positive integers for some fixed $b \geq 2$. More specifically, if $\phi(x)$ is an integer polynomial such that $\phi(n) > 0$ for all $n > 0$, then consider the map $S_{\phi,b} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$, with $S_{\phi,b}(n) := \phi(x_0) + \cdots + \phi(x_d)$ where $n = x_0 + x_1 b + \cdots + x_d b^d$ is the b-ary expansion of n. It is known that the orbit set $\{n, S_{\phi,b}(n), S_{\phi,b}(S_{\phi,b}(n)), \dots\}$ reaches a finite cycle, and for a given b, the union of such cycles over all orbit sets is finite. Fix now an integer $\ell \geq 1$ and let $\phi(x) = x^2$. We show that the set of bases $b \geq 2$ which have at least one cycle of length ℓ always contains an arithmetic progression and thus has positive lower density. We also show that a 1978 conjecture of Hasse and Prichett on the set of bases with exactly two cycles needs to be modified, raising the possibility that there may be infinitely many bases with exactly two cycles.

Index words: Commutative algebra, Commutators, Combinatorics, Algebraic K-theory, Algebraic geometry, Cycle, B-ary expansion, Squared digit sum, Happy number

Two Topics in Algebra and Number Theory

by

Makoto Suwama

B.Sc., University of Sydney, Australia, 2014

A Dissertation Submitted to the Graduate Faculty of the
University of Georgia in Partial Fulfillment of the Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2021

Two Topics in Algebra and Number Theory

by

Makoto Suwama

Major Professor: Dino Lorenzini

Committee: Pete L. Clark

Daniel Litt

Paul Pollack

Electronic Version Approved:

Ron Walcott

Dean of the Graduate School

The University of Georgia

May 2021

Acknowledgments

First and foremost, I would like to express my appreciation to my advisor Dino Lorenzini for his guidance and support throughout my years of study at the University of Georgia. Without him, this dissertation would not have been possible.

I would also like to thank my coauthors Dino, Mentzelos Melistas, Arvind Suresh and Haiyang Wang. The second chapter of the dissertation is based on the paper we worked over the summer of 2020, and the regular Zoom meetings during the midst of the pandemic were helpful keeping me sane and much appreciated.

I have also greatly benefited from many professors in the math department. I would particularly like to thank Valery Alexeev, Pete L. Clark, Daniel Litt, and Paul Pollack for their excellent courses and talks over the years. Their expositions have been exceptional and I have learned much about mathematics as well as how to communicate to an audience effectively.

Last but not least, I am also grateful for the many friends for their support and friendship. I want to especially thank my best friend, Peter Woolfitt, who has always been there for me through thick and thin, cheering me up when I was down and listening to me when I needed to complain.

Contents

List of Tables

Chapter 1

Trace Zero Matrices and Commutators

1.1 Introduction

Let R be a commutative ring. Given two $n \times n$ matrices A and B in $\mathrm{M}_n(R)$, recall that the commutator of A and B is denoted by $[A, B] := AB - BA$. It is a standard fact that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, and since the trace is additive, it follows that $\mathrm{tr}([A, B]) = \mathrm{tr}(AB - BA) = 0$. So it is natural to wonder if the converse is also true. That is, given an $n \times n$ trace 0 matrix C, do there exist two $n \times n$ matrices A and B such that $C = [A, B]$?

The answer to the above question depends on the underlying commutative ring R where the entries lie and the size n of the matrix. If R is a field, then every $n \times n$ trace 0 matrix is a commutator. This was proven by Shoda in [Sho37] for a characteristic 0 field and by Albert and Muckenhoupt in [AM57] for a field with any characteristic.

More recently, Laffey and Reams showed that for every $n \geq 1$, any $n \times n$ trace 0 matrix is a commutator over $R = \mathbb{Z}$ in [LR94], and Stasinski generalised it to an arbitrary principal ideal ring in [Sta16]. Stasinski subsequently showed in [Sta18] that over principal ideal rings, every trace 0 matrix is a commutator of trace

0 matrices as well. In this chapter, we give a new class of rings where every trace 0 matrix is a commutator.

Theorem 1.2.5. *Let R be a Bézout domain with algebraically closed quotient field. Then every trace* 0 *matrix in* $\mathrm{M}_n(R)$ *is a commutator for any* $n \geq 1$.

In Section 1.2, we also discuss hollow matrices and nilpotent matrices which are both special cases of trace 0 matrices, and prove the following theorem.

Theorem 1.2.18. *Let R be a Prüfer domain that is also a k-algebra over an infinite field k. Then for any* $n \geq 1$, *every nilpotent matrix in* $\mathrm{M}_n(R)$ *is a commutator.*

This is a partial progress towards answering whether every $n \times n$ trace 0 matrix over a Dedekind domain is a commutator for any $n \geq 1$. No results for Dedekind domains were previously known for the case when $n \geq 3$ and R is not a principal ideal domain.

On the other hand, there are rings where there is a trace 0 matrix that is not a commutator. Lissner in [Lis61] showed that if R is a polynomial ring in $m \geq 3$ variables, then there is an $n \times n$ trace 0 non-commutator for any $2 \leq n \leq \frac{m+1}{2}$. Mesyan in [Meso6] used a similar idea to create a 2×2 trace 0 non-commutator over a ring with a maximal ideal satisfying certain properties. In Section 1.3 and Section 1.4, we extend the above works of Lissner and Mesyan to construct a trace 0 non-commutator over a more general class of rings.

Theorem 1.3.8. *Let R be a commutative ring with a maximal ideal $\mathfrak{m} \subset R$ such that $R_{\mathfrak{m}}$ is a regular local ring of dimension $m \geq 3$. Suppose further that $n \geq 2$ is an integer such that $n \leq \frac{m^2+2m+5}{8}$. Then there exists a trace* 0 *non-commutator in $M_n(R)$.*

In particular, we improve the bound on the size of the matrix where we can produce a trace 0 non-commutator for a fixed ring; If m is the dimension of the ring and n is the size of the matrix, then Lissner requires $n \leq \frac{m+1}{2}$, so we have improved the bound on the size of the matrix from linear to quadratic in m. This improvement comes from solving a certain combinatorial problem which can be thought of

either as a packing problem or a graph theory problem. The construction of the matrix will be described in Section 1.3, while the combinatorics will be explained in Section 1.4.

In Section 1.5, we give an example of a Noetherian dimension 1 ring where there is an $n \times n$ trace 0 non-commutator for any $n \geq 2$.

Theorem 1.5.2. *There exists a Noetherian commutative domain Λ with dimension 1 such that for every $n \geq 2$, there exists a trace 0 non-commutator in $\mathrm{M}_n(\Lambda)$.*

Finally, in Section 1.6, we discuss 2×2 matrices. The 2×2 matrices are special since every 2×2 trace 0 matrix being a commutator is equivalent to every vector in R^3 being a cross product. This will be discussed further in Section 1.6 along with Theorem 1.6.14 which characterises rings where every 2×2 trace 0 matrix is a commutator. After the characterisation, we prove the following theorem.

Theorem 1.6.23. *Let R be a regular finitely generated $\overline{\mathbb{F}}_p$-algebra of dimension 2. Then R is an OP-ring and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.*

The analogue of the above theorem for $\overline{\mathbb{Q}}$-algebras is also true if the Bloch-Beilinson conjecture holds (see Theorem 1.6.27).

1.2 Bézout Domains and Prüfer Domains

Recall that a *Bézout domain* is a domain where every finitely generated ideal is principal and a *Prüfer domain* is a domain where every finitely generated ideal is invertible. They are non-Noetherian analogues of a PID and a Dedekind domain respectively. A Noetherian Bézout domain is a PID and a Noetherian Prüfer domain is a Dedekind domain. Note that a Bézout domain is a Prüfer domain since principal ideals are always invertible. For a reference on Bézout domains and Prüfer domains see [FS01, Chapter III].

The main idea in this section is about finding an appropriate basis of R^n which puts a given matrix A in a form that makes it easier to show that A is a commutator. We consider A as a matrix over the quotient field K of R to find an appropriate filtration of K^n and then bring down the filtration to R^n to find the

new basis of R^n. We first prove some lemmas related to bringing down a K-vector space filtration to an R-module filtration.

Recall that given an R-module M, there is a natural map $M \to M \otimes_R K$ sending $m \in M$ to $m \otimes 1 \in M \otimes_R K$. If M is torsion-free, then the map is an injection, so we may consider $M \subset M \otimes_R K$ in such a case.

Lemma 1.2.1. *Let R be a domain, K be the quotient field of R and M be a torsion-free R-module. If $U \subset V \subset M \otimes_R K$ are K-subspaces, then $(V \cap M)/(U \cap M)$ is a torsion-free R-module.*

Proof. Let $v \in V \cap M$ and $r \in R$ non-zero such that $rv \in U \cap M$. Then $v \in U$ since $r \neq 0$, and so $v \in U \cap M$. Hence $(V \cap M)/(U \cap M)$ is torsion-free. □

Lemma 1.2.2. *Let R be a Prüfer domain and K be its quotient field. Suppose that M is a finitely generated torsion-free R-module and $U \subset V := M \otimes_R K$ is a K-subspace. Then $U \cap M \subset V$ is a finitely generated R-module.*

Proof. We will prove that $U \cap M$ is finitely generated by inducting on $n := \dim_K V$. If $n = 1$, then $U = \{0\}$ or K, so $U \cap M = \{0\}$ or M, and hence $U \cap M$ is finitely generated.

Suppose it is true for $n - 1$. If $U \cap M = \{0\}$, then we are done, so suppose $U \cap M \neq \{0\}$. Then there exists a non-zero $v \in U \cap M$. Consider the quotient map

$$q : V \to V/Kv.$$

Since M is finitely generated, $q(M) \cong M/(Kv \cap M)$ is also finitely generated, and by Lemma 1.2.1, it is torsion-free as well. Moreover, $M \otimes_R K = V$, so $q(M) \otimes_R K = q(V) \cong K^{n-1}$. We claim that

$$q(U) \cap q(M) = q(U \cap M).$$

Since $q(U) \cap q(M) \supset q(U \cap M)$ is clear, we only show that $q(U) \cap q(M) \subset q(U \cap M)$. So let $x \in q(U) \cap q(M)$. Then there exist $u \in U$ and $m \in M$ such that $x = q(u) = q(m)$. Now

$m - u \in \ker q = Kv \subset U$, so $m = u + (m - u) \in U$ as well, hence $x = q(m) \in q(U \cap M)$. So we have a finitely generated torsion-free module $q(M)$ with $\dim_K q(V) = n - 1$, and so by the inductive hypothesis, $q(M) \cap q(U) = q(U \cap M)$ is a finitely generated R-module. Hence to show that $U \cap M$ is finitely generated, we only need to show that $\ker q \cap (U \cap M) = Kv \cap M$ is finitely generated. Since R is a Prüfer domain, by [FSo1, Theorem V.2.7], there exist finitely generated ideals $I_1, \ldots, I_r \subset R$ such that

$$M \cong I_1 \oplus \cdots \oplus I_r.$$

Suppose $(v_1, \ldots, v_r) \in \oplus_{i=1}^r I_i$ is the image of $v \in M$ under the isomorphism. Then

$$Kv \cap M \cong \{a \in K \mid av \in M\} = \{a \in K \mid av_i \in I_i \ \forall i = 1, \ldots r\} = \bigcap_{i=1}^{r} (I_i : v_i),$$

where $(I_i : v_i) := \{a \in K \mid av_i \in I_i\}$ is the ideal quotient. If $v_i \neq 0$, then $(I_i : v_i) = v_i^{-1} I_i$, so $(I_i : v_i)$ is finitely generated since I_i is finitely generated. If $v_i = 0$, then $(I_i : v_i) = K$. We assumed $v \neq 0$, so at least one $v_i \neq 0$, and so the intersection

$$\bigcap_{i=1}^{r} (I_i : v_i) = \bigcap_{\substack{i=1 \\ v_i \neq 0}}^{r} (I_i : v_i)$$

is non-trivial. Hence $Kv \cap M$ is isomorphic to a finite intersection of finitely generated fractional ideals of a Prüfer domain, so it is finitely generated by [FSo1, Ex. III.1.1] and so we are done. □

Theorem 1.2.3. *Let R be a Bézout domain and K be its quotient field. If the characteristic polynomial of a matrix $A \in \mathrm{M}_n(R)$ splits completely over K, then there exists a basis of R^n such that A is upper triangular with respect to this new basis.*

Proof. If we consider $A \in \mathrm{M}_n(K)$, then since the characteristic polynomial splits completely, there exists a filtration of K-vector spaces

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = K^n,$$

such that $\dim_K V_i = i$ and $AV_i \subset V_i$ for all $i = 1, \ldots, n$ (see e.g. Jordan canonical form in [DF04, p. 12.3]). If we let $W_i := V_i \cap R^n$ for $i = 0, 1, \ldots, n$, then we obtain the following filtration of R-modules

$$0 = W_0 \subset W_1 \subset \cdots \subset W_n = R^n,$$

such that $AW_i \subset W_i$ for all $i = 1, \ldots, n$. By Lemma 1.2.2, W_i's are all finitely generated, hence W_i/W_{i-1}'s are also finitely generated. Now by Lemma 1.2.1, W_i/W_{i-1} is also torsion-free, and so it is a finitely generated torsion-free module over a Bézout domain, hence W_i/W_{i-1} is free by [FS01, Corollary V.2.8]. So the following exact sequence of R-modules splits

$$0 \to W_{i-1} \to W_i \to W_i/W_{i-1} \to 0,$$

and there exists a free rank 1 R-module M_i such that $W_i = W_{i-1} \oplus M_i$. Hence we obtain a decomposition $R^n = \oplus_{i=1}^n M_i$ such that for all $i = 1, \ldots, n$, $AM_i \subset \oplus_{j \leq i} M_j$. Now M_i is a free rank 1 R-module, and so the above decomposition gives an R-basis of R^n such that with respect to this new basis, A is an upper triangular matrix. □

Lemma 1.2.4. *Let R be a ring and $A \in \mathrm{M}_n(R)$ be an upper triangular trace 0 matrix. Then A is a commutator.*

Proof. Let $X = (x_{ij}) \in \mathrm{M}_n(R)$ be the matrix with 1's on the superdiagonal and 0 everywhere else, that is,

$$X = \begin{pmatrix} 0 & 1 & & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

If $A = (a_{ij})$, then we define $B = (b_{ij}) \in \mathrm{M}_n(R)$ sequentially from the top to the bottom as follows:

$$b_{ij} = \begin{cases} 0 & \text{if } i = 1, \\ a_{1,j} & \text{if } i = 2, \\ a_{i-1,j} + b_{i-1,j-1} & \text{if } 3 \leq i \leq n. \end{cases}$$

To ease the notation, we also let $b_{ij} := 0$ if $i = n + 1$ or $j = 0$. Now for any $1 \leq i, j \leq n$, we have

$$[X, B]_{ij} = b_{i+1,j} - b_{i,j-1}.$$

Now for $i = 1$,

$$[X, B]_{1,j} = b_{2,j} - b_{1,j-1} = a_{1,j},$$

and so $[X, B]_{1,j} = A_{1,j}$. For $i \geq 2$, we have

$$[X, B]_{i,j} = b_{i+1,j} - b_{i,j-1} = a_{i,j} + b_{i,j-1} - b_{i,j-1} = a_{i,j},$$

so $[X, B]_{i,j} = A_{i,j}$. Hence $[X, B] = A$. □

We now combine Theorem 1.2.3 and Lemma 1.2.4 to show one of the main theorems of this section.

Theorem 1.2.5. *Let R be a Bézout domain with algebraically closed quotient field. Then every trace 0 matrix in $\mathrm{M}_n(R)$ is a commutator for any $n \geq 1$.*

Proof. By Theorem 1.2.3 we can triangularise A. Note that for any $A \in \mathrm{M}_n(R)$ and $g \in \mathrm{GL}_n(R)$, A is a commutator if and only if gAg^{-1} is a commutator since for any $B, C \in \mathrm{M}_n(R)$,

$$A = [B, C] \iff gAg^{-1} = [gBg^{-1}, gCg^{-1}].$$

Then Lemma 1.2.4 implies that A is a commutator. □

Remark 1.2.6. The only class of rings for which it was previously known that every trace 0 matrix is a commutator is the class of principal ideal rings, and this is due to Stasinski in [Sta16, Theorem 6.3]. So Theorem 1.2.5 gives a new class of rings where every trace 0 matrix is a commutator. Note that Theorem 1.2.5 does not imply Stasinski's result since we assume that the Bézout ring has algebraically closed quotient field. We also note that in our proof, we take a different approach to Stasinski's proof.

We now discuss examples of Bézout domains with algebraically closed quotient field.

Theorem 1.2.7 (Theorem 102 [Kap74])**.** *Let R be a Dedekind domain and K be its quotient field. If for all finite extension L/K, the integral closure S of R in L has torsion Picard group* $\mathrm{Pic}(S)$*, then the integral closure $\overline{R}$ of R in an algebraic closure of K is a Bézout domain.*

Example 1.2.8. Let $R := \mathbb{Z}$ or $R := k[t]$, with k a finite field, and K be the quotient field of R. Then for any finite extension L/K, the integral closure S of R in L has finite Picard group. Hence by Theorem 1.2.7, the integral closure $\overline{R}$ of R in an algebraic closure of K is a Bézout domain. Moreover, the quotient field of $\overline{R}$ is algebraically closed, so by Theorem 1.2.5, every trace 0 matrix is a commutator over $\overline{R}$.

Corollary 1.2.9. *Let R be a Dedekind domain and K be its quotient field. If for all finite extension L/K, the integral closure S of R in L has torsion Picard group* $\mathrm{Pic}(S)$*, then for all trace* 0 *matrix $A \in \mathrm{M}_n(R)$, there exists an R-algebra T such that T is finitely generated as an R-module and A is commutator in* $\mathrm{M}_n(T)$*.*

Proof. By Theorem 1.2.7, the integral closure $\overline{R}$ of R in an algebraic closure of K is a Bézout domain. Hence by Theorem 1.2.5, A is a commutator over $\overline{R}$, so $A = [B, C]$ for some $B, C \in \mathrm{M}_n(\overline{R})$. If we take $T := R[b_{ij}, c_{ij} : 1 \leq i, j \leq n] \subset \overline{R}$, then $B, C \in \mathrm{M}_n(T)$, so A is a commutator in $\mathrm{M}_n(T)$. □

Remark 1.2.10. In Corollary 1.2.9, we could also take the integral closure T' of R in the quotient field F of T. Then T' will be a Dedekind domain, but not necessary finitely generated R-module, unless F/K is separable or R is finitely generated over a field.

We now discuss the case of hollow endomorphisms of R-modules for an arbitrary ring R, and then specialise it to nilpotent matrices over Prüfer domain in Theorem 1.2.18. Recall that an $n \times n$ matrix is

hollow if all of its diagonal entries are zero (see e.g. [Gen17, p. 3.1] for a reference on hollow matrices). In the following definition, we generalise the concept of a hollow matrix to an endomorphism of an arbitrary R-module with a decomposition.

Definition 1.2.11. Let R be a ring and M be an R-module. Suppose we have a decomposition $M = \oplus_{k=1}^{n} M_k$ where $M_k \subset M$ are R-submodules. Then for any $A \in \mathrm{End}_R(M)$ and $1 \leq i, j \leq n$, define $a_{ij} := \pi_i A \iota_j \in \mathrm{Hom}_R(M_j, M_i)$, where $\pi_i \in \mathrm{Hom}_R(\oplus_{k=1}^{n} M_k, M_i)$ is the projection and $\iota_j \in \mathrm{Hom}_R(M_j, \oplus_{k=1}^{n} M_k)$ is the inclusion. We can think of (a_{ij}) as an $n \times n$ matrix where the (i, j)-th entry a_{ij} lies in $\mathrm{Hom}_R(M_j, M_i)$ instead of R. We say that $A \in \mathrm{End}_R(M)$ is *hollow with respect to a decomposition* $M = \oplus_{k=1}^{n} M_k$ if $a_{kk} = 0$ for all $k = 1, \ldots, n$.

Note that a matrix $A \in \mathrm{M}_n(R)$ being hollow is the same as $A \in \mathrm{End}_R(R^n)$ being a hollow endomorphism with respect to the decomposition coming from the standard basis.

Let R be a commutative ring with $C := \{r_1, \ldots, r_n\} \subset R^\times$ such that $r_i - r_j \in R^\times$ for all $i \neq j$. Such a set C is called a *clique of exceptional units*. This term is usually used in the context of number rings, and the cliques were used by Lenstra to construct Euclidean fields in [Len77].

Example 1.2.12. Let k be a field and R be a k-algebra. Then any $C \subset k^\times \subset R^\times$ is a clique of exceptional units since $x - y \in k^\times \subset R^\times$ for all distinct $x, y \in C$.

Theorem 1.2.13. *Let R be a commutative ring with a clique of exceptional units $\{r_1, \ldots, r_n\}$ of size $n \geq 1$. Let M be a finitely generated R-module with a decomposition $M = \oplus_{k=0}^{n} M_k$, and suppose that $A \in \mathrm{End}_R(M)$ is hollow with respect to that decomposition. Then*

$$A = [X, A']$$

for some $X, A' \in \mathrm{End}_R(M)$. In particular, every hollow matrix in $\mathrm{M}_{n+1}(R)$.

Proof. Let X be the diagonal matrix with $r_0 := 0, r_1, \ldots, r_n$ on the diagonal. We slightly abuse notation here and we denote by r_i the element in R and the endomorphism given by multiplication by r_i on M_i so

that we can view X as an element of $\mathrm{End}_R(M)$. If $A = (a_{ij})$, then define $A' := (a'_{ij}) \in \mathrm{End}(\oplus_{k=0}^n M_k)$ as follows:

$$a'_{ij} := \begin{cases} 0 & \text{if } i = j \\ (r_i - r_j)^{-1} a_{ij} & \text{otherwise} \end{cases}.$$

Note that $r_1, \ldots, r_n$ are units, so $r_0 - r_i = -r_i$ is a unit for all $1 \leq i \leq n$. Then

$$[X, A']_{ij} = x_{ii}a'_{ij} - a'_{ij}x_{jj} = r_i a'_{ij} - a'_{ij} r_j = (r_i - r_j)a'_{ij} = a_{ij},$$

so $A = [X, A']$.

The last part follows since a hollow matrix $A \in \mathrm{M}_{n+1}(R)$ is hollow with respect to the decomposition of R^{n+1} coming from the standard basis. □

Corollary 1.2.14. *Let k be a field and R be a k-algebra. Then every hollow matrix in $\mathrm{M}_n(R)$ is a commutator for any $1 \leq n \leq \#k$. In particular, if k is a field of infinite cardinality, then every $n \times n$ hollow matrix is a commutator for any $n \geq 1$.*

Proof. From Example 1.2.12, we have a clique of exceptional units $C \subset k^\times \subset R^\times$ of any size up to $\#k^\times$. Since every hollow matrix in $\mathrm{M}_{\#C+1}(R)$ is a commutator by Theorem 1.2.13, every $n \times n$ hollow matrix is a commutator for any $1 \leq n \leq \#k^\times + 1 = \#k$. □

We now consider nilpotent matrices over a Prüfer domain R. We generalise the procedure described by Appleby in [App98, Section 3] from Dedekind domains to Prüfer domains. This allows us to find a decomposition of a finitely generated torsion-free R-module M that makes A strictly upper triangular for any fixed nilpotent endomorphism $A \in \mathrm{End}_R(M)$.

Lemma 1.2.15. *Let R be a Prüfer domain, M be a finitely generated torsion-free R-module and $A \in \mathrm{End}_R(M)$ be a nilpotent endomorphism. Then there exists a decomposition $M = \oplus_{i=1}^n M_i$ where $n = \mathrm{rk}\, M$, such that the endomorphism A is strictly upper triangular with respect to this decomposition.*

Proof. Let K be the quotient field of R and $V := M \otimes_R K$. Then $M \subset V$ since M is torsion-free, and we can consider $A \in \mathrm{End}_K(V)$. Since A is nilpotent, we can find a filtration of K-vector spaces

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V,$$

such that $AV_i \subset V_{i-1}$ for all $i = 1, \ldots, n$, and $\dim_K V_i = i$. If we let $W_i := R^n \cap V_i$ for $i = 1, \ldots, n$, then we obtain the following filtration of R-modules

$$0 = W_0 \subset W_1 \subset \cdots \subset W_n = M,$$

such that $AW_i \subset W_{i-1}$ for all $i = 1, \ldots, n$. Now, W_i is a finitely generated R-module by Lemma 1.2.2, and so W_i/W_{i-1} is also finitely generated. Now by Lemma 1.2.1, W_i/W_{i-1} is a torsion-free as well, and so it is a finitely generated torsion-free module over a Prüfer domain, hence projective by [FS01, Theorem V.2.7]. So the following exact sequence splits,

$$0 \to W_{i-1} \to W_i \to W_i/W_{i-1} \to 0,$$

and we have $W_i = W_{i-1} \oplus M_i$ for some R-module M_i. So we obtain a decomposition $M = \oplus_{i=1}^n M_i$. Now consider the matrix representation $A = (a_{ij})$ with respect to this decomposition. Then $a_{ij} = 0$ for all $1 \leq j \leq i \leq n$ since $AM_j \subset W_{j-1}$ and $W_{j-1} \cap M_i = 0$. Hence A is strictly upper triangular with respect to the decomposition $M = \oplus_{i=1}^n M_i$. □

Remark 1.2.16. For a commutative Noetherian ring R, Yohe showed that every nilpotent matrix being similar to a strictly upper triangular matrix is equivalent to R being a principal ideal ring [Yoh67, Theorem 1]. So for a non-PID Dedekind domain R, there are nilpotent matrices that are not similar to a strictly upper triangular matrix. Nevertheless, in Lemma 1.2.15, we show that by allowing the matrix entries to lie in $\mathrm{Hom}_R(M_j, M_i)$ instead of R, we can put any nilpotent matrix over R in a strictly upper triangular form.

Corollary 1.2.17. *Let R be a Prüfer domain with a clique of exceptional units $C := \{r_1, \ldots, r_n\}$ of size $n \geq 1$, and M be a finitely generated projective R-module M of rank $m \leq n+1$. Then every nilpotent endomorphism $A \in \mathrm{End}_R(M)$ is a commutator. In particular, every nilpotent matrix in $\mathrm{M}_m(R)$ is a commutator for all $1 \leq m \leq n+1$.*

Proof. By Lemma 1.2.15, we can construct a decomposition $M = \oplus_{k=1}^{m} M_k$ such that A is hollow with respect to this decomposition. Since any subset of a clique of exceptional units is still a clique, we can take a subset of C of size $m-1$ and apply Theorem 1.2.13 to obtain $X, A' \in \mathrm{End}_R(M)$ such that $A = [X, A']$. □

Theorem 1.2.18. *Let R be a Prüfer domain that is also a k-algebra over an infinite field k. Then for any $n \geq 1$, every nilpotent matrix in $\mathrm{M}_n(R)$ is a commutator.*

Proof. From Example 1.2.12, we have a clique of exceptional units $k^\times \subset R^\times$. So by Corollary 1.2.17, every nilpotent endomorphism in $\mathrm{End}_R(M)$ is a commutator if $\mathrm{rk}\, M \leq \#k^\times + 1 = \#k$. □

Theorem 1.2.18 provides partial progress towards answering the following open question.

Question 1.2.19 (Section 7 [Sta16])**.** Let R be a Dedekind domain and $n \geq 3$. Is every $n \times n$ trace 0 matrix in $\mathrm{M}_n(R)$ a commutator?

Note that a Dedekind domain is a Prüfer domain. Lissner answered Question 1.2.19 affirmatively in [Lis65, Appendix] for $n = 2$, but no progress has been made since for $n \geq 3$.

Example 1.2.20. For a fixed n, we can provide examples of non-PID number rings R where every nilpotent matrix in $\mathrm{M}_m(R)$ is commutator for all $1 \leq m \leq n$. We construct a large clique of exceptional units in $\mathbb{Z}[\zeta_p]$ for a prime p where $\zeta_p = e^{2\pi i/p}$ based on an example in [Len77, Section 3]. Let $\omega_i := \frac{\zeta_p^i - 1}{\zeta_p - 1} \in \mathbb{Z}[\zeta_p]$ for any $i = 1, \ldots, p-1$. Then the absolute norm of ω_i is 1, so $\omega_i \in \mathbb{Z}[\zeta_p]^\times$ for all $i = 1, \ldots, p-1$. Now given $1 \leq i < j \leq p-1$,

$$\omega_j - \omega_i = \zeta_p^i \omega_{j-i} \in \mathbb{Z}[\zeta_p]^\times,$$

so $\{\omega_1, \ldots, \omega_{p-1}\}$ is a clique of exceptional units. Hence by Corollary 1.2.17, every nilpotent matrix in $\mathrm{M}_m(\mathbb{Z}[\zeta_p])$ is a commutator for all $1 \leq m \leq p$. Moreover, $\mathbb{Z}[\zeta_p]$ has class number greater than 1 for all primes $p \geq 23$ (see [Was97, Theorem 11.1]), so $\mathbb{Z}[\zeta_p]$ will not be a PID for those primes. Hence for any prime $p \geq 23$, $\mathbb{Z}[\zeta_p]$ gives a non-trivial example which does not follow from [Sta16, Theorem 6.3].

Remark 1.2.21. Lenstra in [Len77, Corollary 1.8] showed that if a number ring R admits a clique of exceptional units of sufficiently large size relative to the degree and the discriminant, then R must be an Euclidean domain. In which case R is also a PID and Corollary 1.2.17 is then not needed since we know that every trace 0 matrix over a PID is a commutator by [Sta16, Theorem 6.3].

1.3 Construction of Trace Zero Non-commutators

In this section, we construct a trace 0 non-commutator assuming we can solve a certain combinatorial problem which is stated in Question 1.4.1 in the next section. We will first give a couple of definitions that will be used in the problem and the main theorem Theorem 1.3.3.

Definition 1.3.1. Let $m \geq 1$ and $d \geq 0$ be integers. We will call a set $S \subset \mathbb{Z}_{\geq 0}^m$ *d-separated* if for all distinct $s = (s_i), s' = (s'_i) \in S$,

$$|s - s'|_1 := \sum_{i=1}^{m} |s_i - s'_i| > d.$$

Definition 1.3.2. Let $n, r \in \mathbb{Z}_{\geq 0}$. Then the *discrete n-simplex of length r* is

$$\Delta(n, r) := \left\{ v = (v_i) \in \mathbb{Z}_{\geq 0}^{n+1} \;\middle|\; \sum_{i=1}^{n+1} v_i = r \right\}.$$

We now give the construction of the trace 0 non-commutator. Let R be a commutative ring. We use the following notation in the theorem: given a point $s = (s_i) \in \mathbb{Z}_{\geq 0}^m$ and elements $x_1, \ldots, x_m \in R$, we let $x^s := \prod_{i=1}^m x_i^{s_i} \in R$. As usual, we set $r^0 := 1$ for any $r \in R$.

Theorem 1.3.3. *Let R be a commutative ring with an ideal $I \subset R$ with the following property: there exist non-zero $x_1, \ldots, x_m \in I$ with $m \geq 3$, and $d \geq 0$ such that for all $0 \leq k \leq 3d+1$,*

$$I^k/I^{k+1} = \bigoplus_{\substack{t \in \mathbb{Z}^m_{\geq 0} \\ |t|_1 = k}} (R/I)(x^t + I^{k+1}).$$

In other words, I^k/I^{k+1} is a free R/I-module and the degree k monomials in the x_i's form an R/I-basis of I^k/I^{k+1} for all $0 \leq k \leq 3d+1$.

Suppose further that there exists a $2d$-separated set $S := \{s_1, \ldots, s_{2n-1}\} \subset \Delta(m-1, 2d+1) \subset \mathbb{Z}^m_{\geq 0}$ with $n \geq 2$. Then

$$X := \begin{pmatrix} x^{s_1} & x^{s_2} & \cdots & x^{s_{n-1}} & x^{s_n} \\ x^{s_{n+1}} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x^{s_{2n-2}} & 0 & \cdots & 0 & 0 \\ x^{s_{2n-1}} & 0 & \cdots & 0 & -x^{s_1} \end{pmatrix}$$

is a trace 0 non-commutator in $\mathrm{M}_n(R)$.

Proof. Since $\mathrm{tr}(X) = x^{s_1} - x^{s_1} = 0$, the only remaining thing we need to show is that X is not a commutator. Suppose by contradiction that $X = [B, C]$ for some $B = (b_{ij}), C = (c_{ij}) \in M_n(R)$. Then

$$[B - b_{nn}I_n, C - c_{nn}I_n] = [B, C] = X,$$

so we may assume $b_{nn} = 0 = c_{nn}$ by taking $B - b_{nn}I_n$ and $C - c_{nn}I_n$.

Now suppose $b_{i1}, b_{1i}, c_{i1}, c_{1i} \in I^{d+1}$ for all $i = 1, \ldots, n$. Then from $X = [B, C]$, we have

$$a_{11} = \sum_{i=1}^{n} (b_{1i}c_{i1} - c_{1i}b_{i1}) \in I^{2d+2}.$$

But $a_{11} = x^{s_1} \in I^{2d+1}$ is part of the R/I-basis of I^{2d+1}/I^{2d+2}, so $a_{11} \notin I^{2d+2}$, which is a contradiction. Hence to show that X is a non-commutator, we only need to show that $b_{i1}, b_{1i}, c_{i1}, c_{1i} \in I^{d+1}$ for all i.

We will first show that $b_{i1}, b_{1i} \in I^{d+1}$ for all i. So let k be the minimum integer such that $b_{i1} \in I^k \setminus I^{k+1}$ or $b_{1i} \in I^k \setminus I^{k+1}$ for some i. If $k \geq d+1$ or no such k exists then we are done so assume $k \leq d$. Without loss of generality, assume that $b_{1j} \in I^k \setminus I^{k+1}$. Then writing b_{1j} in terms of the monomial basis in I^k/I^{k+1}, we have

$$b_{1j} \equiv \sum_{t \in \Delta(m-1,k)} r_t x^t \mod I^{k+1},$$

with $r_t \in R$ for all $t \in \Delta(m-1,k) \subset \mathbb{Z}^m_{\geq 0}$ such that $r_{t_0} \notin I$ for some $t_0 \in \Delta(m-1,k)$. Now from $X = [B, C]$, we have

$$\operatorname{tr}(BX) = \operatorname{tr}(B[B,C]) = \operatorname{tr}(BBC - BCB) = \operatorname{tr}([B, BC]) = 0.$$

Since $b_{nn} = 0$, we have

$$0 = \operatorname{tr}(BX) = \sum_{i=0}^{n} \sum_{j=0}^{n} b_{ij} a_{ji} = a_{11} b_{11} + \sum_{i=2}^{n} b_{i1} a_{1i} + \sum_{j=2}^{n} b_{1j} a_{j1}. \tag{1.1}$$

Now, $a_{1j} = x^{s_j}$ with $|s_j|_1 = 2d+1$, so

$$a_{1j} b_{j1} = x^{s_j} b_{j1} \equiv \sum_{t \in \Delta(m-1,k)} r_t x^{s_j + t} \in I^{k+2d+1}/I^{k+2d+2}.$$

Now $r_{t_0} \in R \setminus I$, and so by considering eq. (1.1) mod I^{k+2d+2}, we see that a term with a monomial $x^{s_j+t_0}$ must also appear in $b_{1i}a_{i1}$ or $b_{i1}a_{1i}$ mod I^{k+2d+2} for some i. So suppose $b_{i1}a_{1i}$ contains such a term. Then we have $x^{s_j+t_0} \equiv x^u x^{s_i} \mod I^{k+2d+2}$ where x^u comes from b_{i1} and $|u|_1 = k$. So we have $s_j + t_0 = u + s_i$ which implies

$$|s_i - s_j| = |t_0 - u| \leq |t_0| + |u| = 2k \leq 2d.$$

This is a contradiction since S is $2d$-separated. Hence $k \geq d+1$, and so $b_{1i}, b_{i1} \in I^{d+1}$ for all i. By similar argument, $c_{1i}, c_{i1} \in I^{d+1}$ as well. Hence no such matrices B and C can exist and X is a non-commutator. □

The following corollary generalises the result of Mesyan [Meso6, Prop. 20].

Corollary 1.3.4. *Let R be a ring and suppose that $I := (x_1, \ldots, x_m)$ is an ideal such that I/I^2 is a free R/I-module with the classes of $x_1, \ldots, x_m$ in I/I^2 forming an R/I-basis. Then for any $2 \leq n \leq \frac{m+1}{2}$,*

$$X := \begin{pmatrix} x_1 & x_2 & \cdots & x_{n-1} & x_n \\ x_{n+1} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{2n-2} & 0 & \cdots & 0 & 0 \\ x_{2n-1} & 0 & \cdots & 0 & -x_1 \end{pmatrix}$$

is not a commutator in $\mathrm{M}_n(R)$. In particular, if a Noetherian ring R has Krull dimension $m \geq 3$, then there exists a trace 0 non-commutator in $\mathrm{M}_n(R)$ for any $2 \leq n \leq \frac{m+1}{2}$.

Proof. We will use Theorem 1.3.3 to construct the trace 0 non-commutator. If we take $d = 0$, then the basis condition in the theorem is equivalent to I/I^2 being a free R/I-module. For the set S in the theorem, if $d = 0$ then any set $S \subset \Delta(m-1, 1)$ is automatically $2d$-separated. Hence we can take S to be $\Delta(m-1,1) = \{e_1, \ldots, e_m\} \subset \mathbb{Z}^m_{\geq 0}$ where e_i's are the standard basis of $\mathbb{Z}^m$. Now if $n \leq \frac{m+1}{2}$, then we may take $2n-1$ points inside $\Delta(m-1,1)$. Hence by Theorem 1.3.3, X is a non-commutator. The second part follows since if we take $I \subset R$ to be a maximal ideal with maximum height, then $\dim_{R/I} I/I^2 \geq \dim R = m$ (see Theorem 13.5 in [Mat89]). □

Remark 1.3.5. Let R be a ring and $\mathfrak{m} \subset R$ be a maximal ideal such that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \geq 3$. Then by Corollary 1.3.4, there exists a trace 0 non-commutator in $\mathrm{M}_2(R)$. This also follows from [Meso6, Prop. 20]. Such a maximal ideal exists if R is a Noetherian integrally closed domain of dimension 2 that is not regular. Indeed, by Serre's criterion [Mat89, Theorem 23.8], R being integrally closed implies $R_{\mathfrak{p}}$ is regular

for any prime ideal $\mathfrak{p} \subset R$ with $\mathrm{ht}(\mathfrak{p}) \leq 1$. But R is not regular, so $R_{\mathfrak{m}}$ must be singular at some maximal ideal $\mathfrak{m} \subset R$ of $\mathrm{ht}(\mathfrak{m}) = 2$. At such maximal ideal $\mathfrak{m}$, $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 > \dim R_{\mathfrak{m}} = \mathrm{ht}(\mathfrak{m}) = 2$ and so there exists a trace o non-commutator in $\mathrm{M}_2(R)$.

The following result of Lissner is a special case of Corollary 1.3.4.

Corollary 1.3.6 (Theorem 5.4 [Lis61])**.** *Let K be a field, $n \geq 2$ be an integer and $R = K[x_1, \ldots, x_m]$, with $m \geq 2n - 1$. Then there exists a trace 0 non-commutator in $\mathrm{M}_n(R)$.*

We now demonstrate that the condition in Theorem 1.3.3 about the structure of I^k/I^{k+1} is relatively easy to satisfy. The following lemma gives a large class of a ring and an ideal satisfying the condition. Recall that given a commutative ring R and an ideal $I \subset R$, we can construct the *associated graded ring* $\mathrm{gr}_I(R) := \oplus_{i \geq 0} I^i/I^{i+1}$. Then given an element $r \in R$, we can associate an element $\mathrm{in}(r) \in \mathrm{gr}_I(R)$ called the *initial form* defined as follows. Let $j \geq 0$ be such that $r \in I^j \setminus I^{j+1}$. If no such j exists, then $r \in \cap_i I^i$, and we take $\mathrm{in}(r) := 0 \in \mathrm{gr}_I(R)$. Otherwise take $\mathrm{in}(r) := r + I^{j+1} \in I^j/I^{j+1} \subset \mathrm{gr}_I(R)$.

Lemma 1.3.7. *Let R be a ring and $\mathfrak{m} \subset R$ be a maximal ideal such that $R_{\mathfrak{m}}$ is a regular local ring (see [Mat89, Section 14] for the definition of a regular local ring). Then*

$$\mathrm{gr}_{\mathfrak{m}}(R) \cong k_{\mathfrak{m}}[x_1, \ldots, x_m],$$

where $k_{\mathfrak{m}} := R/\mathfrak{m}$ is the residue field and m is the dimension of $R_{\mathfrak{m}}$ (which is finite since $R_{\mathfrak{m}}$ is a Noetherian local ring) and $k_{\mathfrak{m}}[x_1, \ldots, x_m]$ is a polynomial ring in m variables. Moreover, there exist $y_1, \ldots, y_m \in \mathfrak{m}$ such that $\mathrm{in}(y_1), \ldots, \mathrm{in}(y_m)$ map to $x_1, \ldots, x_m$ under the above isomorphism and the degree k monomials in the y_i's form a $k_{\mathfrak{m}}$-basis of $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ for all $k \geq 0$.

Proof. Since $R_{\mathfrak{m}}$ is a regular local ring,

$$\mathrm{gr}_{\mathfrak{m}R_{\mathfrak{m}}}(R_{\mathfrak{m}}) \cong k_{\mathfrak{m}}[x_1, \ldots, x_m],$$

as graded rings by Theorem 14.4 in [Mat89]. Now $\mathfrak{m}$ is maximal, so $\mathfrak{m}^i/\mathfrak{m}^{i+1} \cong (\mathfrak{m}R_\mathfrak{m})^i/(\mathfrak{m}R_\mathfrak{m})^{i+1}$ for all $i \geq 0$, and hence $\mathrm{gr}_\mathfrak{m}(R) \cong \mathrm{gr}_{\mathfrak{m}R_\mathfrak{m}}(R_\mathfrak{m})$. So we have

$$\mathrm{gr}_\mathfrak{m}(R) \cong \mathrm{gr}_{\mathfrak{m}R_\mathfrak{m}}(R_\mathfrak{m}) \cong k_\mathfrak{m}[x_1, \ldots, x_m].$$

They are isomorphic as graded rings, so there exist $y_1, \ldots, y_m \in R$ such that $\mathrm{in}(y_i)$ maps to x_i. The above isomorphism also implies that the degree k monomials in y_i's form a $k_\mathfrak{m}$-basis of $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ for all $k \geq 0$ since it is true for the polynomial ring on the right hand side. □

We now state the main result combining Theorem 1.3.3 and the combinatorial result Theorem 1.4.10.

Theorem 1.3.8. *Let R be a commutative ring with a maximal ideal $\mathfrak{m} \subset R$ such that $R_\mathfrak{m}$ is a regular local ring of dimension $m \geq 3$. Suppose further that $n \geq 2$ is an integer such that $n \leq \frac{m^2+2m+5}{8}$. Then there exists a trace 0 non-commutator in $M_n(R)$.*

Proof. We will use Theorem 1.3.3 to construct the trace 0 non-commutator, so we need to check the basis condition, and construct the set S in the assumption of the theorem. By Lemma 1.3.7, the basis condition in Theorem 1.3.3 is satisfied for all d, and by Theorem 1.4.10, if m is odd, then there exists an S with $\#S = \frac{(m+1)^2}{4}$. So if $2n-1 \leq \frac{(m+1)^2}{4}$, then the assumption of Theorem 1.3.3 is satisfied and there exists a trace 0 non-commutator in $M_n(R)$. If we rearrange $2n-1 \leq \frac{(m+1)^2}{4}$, we obtain $n \leq \frac{m^2+2m+5}{8}$. For m even, there exists an S with $\#S = 2n-1 \leq \frac{m(m+2)}{4}$ from Theorem 1.4.10, and we may rearrange the inequality to $n \leq \frac{m^2+2m+4}{8}$. But if m is even and n is an integer, then $n \leq \frac{m^2+2m+4}{8}$ is equivalent to $n \leq \frac{m^2+2m+5}{8}$ so we have the stated inequality for m even as well. □

For an ideal I of a ring R, let $\nu(I)$ be the minimal number of generators of I. In the case of a Noetherian local ring R and its maximal ideal $\mathfrak{m}$, we have $\nu(\mathfrak{m}) = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$ by Nakayama's Lemma [Mat89, Theorem 2.3].

Corollary 1.3.9. *Let R be a Noetherian ring and let $n \geq 2$ be such that every trace 0 matrix in $\mathrm{M}_n(R)$ is a commutator. Then for all maximal ideals $\mathfrak{m}$ of R,*

$$\nu(\mathfrak{m}) < \begin{cases} 2\sqrt{2n-1} & \text{if } R_{\mathfrak{m}} \text{ is regular,} \\ 2n-1 & \text{otherwise.} \end{cases}$$

Proof. Suppose $R_{\mathfrak{m}}$ is regular. Since every $n \times n$ trace 0 matrix is a commutator, $n > \frac{m^2+2m+5}{8}$ where $m = \dim R_{\mathfrak{m}} = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = \nu(\mathfrak{m}R_{\mathfrak{m}})$ by Theorem 1.3.8. Hence $2\sqrt{2n-1} - 1 > m = \nu(\mathfrak{m}R_{\mathfrak{m}})$. Now by [DG77, Theorem 1], $\nu(\mathfrak{m}R_{\mathfrak{m}}) + 1 \geq \nu(\mathfrak{m})$ if $R_{\mathfrak{m}}$ is regular, so

$$2\sqrt{2n-1} > \nu(\mathfrak{m}).$$

Hence the stated inequality follows.

For $R_{\mathfrak{m}}$ not regular, we apply Corollary 1.3.4 to obtain $n > \frac{m+1}{2}$ where $m = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = \nu(\mathfrak{m}R_{\mathfrak{m}})$. Hence

$$2n-1 > m = \nu(\mathfrak{m}R_{\mathfrak{m}}).$$

Now by [DG77, Theorem 1], $\nu(\mathfrak{m}R_{\mathfrak{m}}) = \nu(\mathfrak{m})$ if $R_{\mathfrak{m}}$ is not regular, so the stated inequality follows. □

Remark 1.3.10. If R is a Noetherian ring such that every 2×2 trace 0 is a commutator, then Corollary 1.3.9 implies

$$\nu(\mathfrak{m}) \leq \begin{cases} 3 & \text{if } R_{\mathfrak{m}} \text{ is regular,} \\ 2 & \text{otherwise,} \end{cases}$$

for any maximal ideal $\mathfrak{m} \subset R$. However, it is known that $\nu(\mathfrak{m}) \leq 2$ for any maximal ideal $\mathfrak{m}$ if every 2×2 trace 0 matrix is a commutator (see Lemma 1.6.11). Note that even when $n = 2$ and $\nu(\mathfrak{m}) \leq 2$ for all maximal ideals $\mathfrak{m}$, the converse of Corollary 1.3.9 does not hold. See however, Theorem 1.6.5 and Corollary 1.6.18 for a partial converse.

In view of Theorem 1.3.8, it is natural to ask the following question.

Question 1.3.11. Let R be a Noetherian ring such that there exists $c > 0$ with $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \leq c$ for all maximal ideals $\mathfrak{m} \subset R$. Does there exist an $n_0 = n_0(R) \geq 1$ such that for all $n \geq n_0$, every trace 0 matrix in $\mathrm{M}_n(R)$ is a commutator?

The example produced in Theorem 1.5.2 shows that the answer to this question is negative if the assumption on the existence of such c is omitted. The simplest rings for which the question is open are regular local rings of dimension 2 and Dedekind domains. For both of those types of rings, it is not known whether every $n \times n$ trace 0 matrix is a commutator for any $n \geq 3$.

Let us now summarise below the largest trace 0 non-commutator we can construct for a fixed ring and an ideal using Theorem 1.3.3.

Theorem 1.3.12. *Let R be a polynomial ring in $m \geq 3$ variables over a field and $d \geq 0$ or, more generally, let R be a ring with an ideal $I \subset R$ satisfying the basis condition from Theorem 1.3.3. That is, there exist some non-zero $y_1, \ldots, y_m \in I$ with $m \geq 3$ such that the degree k monomials in the y_i's form an R/I-basis of I^k/I^{k+1} for all $0 \leq k \leq 3d+1$. Then the following list describes the sizes n for which we can construct a trace 0 non-commutator in $\mathrm{M}_n(R)$.*

1. *If $d = 0$, then any $2 \leq n \leq \frac{m+1}{2}$.*
2. *If $d = 1$ and $m \not\equiv 5 \pmod 6$, then any $2 \leq n \leq \frac{1}{2}(\lfloor \frac{m}{3} \lfloor \frac{m-1}{2} \rfloor \rfloor + m + 1)$.*
3. *If $d = 1$ and $m \equiv 5 \pmod 6$, then any $2 \leq n \leq \frac{1}{2}(\lfloor \frac{m}{3} \lfloor \frac{m-1}{2} \rfloor \rfloor + m)$.*
4. *If $m = 3$, then $n = 2$.*
5. *If $m \geq 4$ and $d \geq m-1$, then any $2 \leq n \leq \frac{m^2+2m+5}{8}$.*
6. *For certain specific m and d, the corresponding entry in the table below is the size of the largest non-commutator matrix that Theorem 1.3.3 can construct. When the entry is in bold, it is bigger than the upperbound provided by (5).*

Table 1.1: Size of the largest non-commutator matrix that Theorem 1.3.3 can construct

m \ d	2	3	4	5	6	7	8	9	10	11	12
4	3	3	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**	**4**
5	5	5	5	**6**	**6**	**6**	**6**	**6**	**7**		
6	6	7	**8**								
7	9										
8	12										

Proof. We will use Theorem 1.3.3 to construct the trace 0 non-commutator.

For (1), the proof is in Corollary 1.3.4. Note that the assumptions of the Theorem 1.3.3 can be simplified to the assumptions in Corollary 1.3.4 (see the proof of Corollary 1.3.4 for more details on the assumptions).

For (2) to (6) we will first describe the set S used in Theorem 1.3.3.

For (2) and (3) we will use Theorem 1.4.6. Given $d = 1$ and $m \geq 0$, take S to be the maximum set of binary vectors of length m that are Hamming distance at least 4 apart and constant weight 3.

For (4), Proposition 1.4.7 describes how to obtain the set S for $m = 3$ and for any d. For (5), Theorem 1.4.10 describes how to obtain the set S for any $m \geq 1$ and $d \geq m - 1$. For (6) Proposition 1.4.8 describes the largest S one can obtain for the listed m and d.

Once the S needed for Theorem 1.3.3 is obtained, we can construct an $n \times n$ trace 0 non-commutator if $2n - 1 \leq \#S$. Note that for (5), we have $\#S = \frac{m(m+2)}{4}$ when m is even. This inequality can be rearranged to $2 \leq n \leq \frac{m^2+2m+4}{8}$, but this is equivalent to $2 \leq n \leq \frac{m^2+2m+5}{8}$ since m is even. Hence we obtain the inequality stated in (5) for both even and odd m. □

Remark 1.3.13. The n's given in the table in Theorem 1.3.12 is the largest size for which we can construct a trace 0 non-commutator using Theorem 1.3.3. On the other hand, (5) in the list can be improved if we can construct a bigger S required for Theorem 1.3.3. For example, if $m = 4$, (5) gives $2 \leq n \leq 3$, but we see that in the table in (6), we can take $n = 4$ if $d \geq 4$.

While the upper bound on n in Theorem 1.3.8 could be improved, the size of the non-commutator we can construct using Theorem 1.3.3 is bounded for a fixed ring R and ideal $I \subset R$, as we now show.

Proposition 1.3.14. *Let R be a commutative ring and let $I \subset R$ be an ideal such that I/I^2 is a free R/I-module with rank $m \geq 3$. Then the size n of a trace 0 non-commutator one can construct using Theorem 1.3.3 is bounded above by 2^{2m-3}.*

Proof. If m is finite, then the size of the set $S = \{s_1, \ldots, s_{2n-1}\}$ required in Theorem 1.3.3 is bounded above by 4^{m-1} by Corollary 1.4.15. So we have $2n - 1 \leq 4^{m-1}$ which implies $n \leq 2^{2m-3}$. Hence the largest trace 0 non-commutator one can construct using Theorem 1.3.3 is bounded above by 2^{2m-3}. □

Remark 1.3.15. Proposition 1.3.14 gives an upperbound for the size of the non-commutator one can construct using Theorem 1.3.3 for a fixed R and I. However, if we only fix R, then the size of the non-commutator can be arbitrary large in general. We will later construct a ring with such a property in Theorem 1.5.2.

1.4 Combinatorics

We will now discuss the set S required in Theorem 1.3.3. Namely, we would like to answer the following questions.

Question 1.4.1. Given $m \geq 1$ and $d \geq 0$, how large can a set $S \subset \mathbb{Z}^m_{\geq 0}$ be if it is $2d$-separated and contained in $\Delta(m-1, 2d+1)$?

Question 1.4.2. Given $m \geq 1$, how large can a set S be if it is $2d$-separated and contained in $\Delta(m-1, 2d+1) \subset \mathbb{Z}^m_{\geq 0}$ for some $d \geq 0$?

An answer for Question 1.4.1 will give the size of the largest matrix we can construct using Theorem 1.3.3 for a fixed m and d. While an answer to Question 1.4.2 will be useful in the situation of Lemma 1.3.7 where we are allowed to take arbitrary large d.

To answer the above questions, we will first use the following lemma to simplify the problem.

Lemma 1.4.3. *Let $m \geq 1$ and $d \geq 0$ be integers, and suppose that a set S is $2d$-separated and contained in $\Delta(m-1, 2d+1)$. Then there exists a set S' such that S' is $2d$-separated, contained in $\Delta(m-1, 2d+1)$, $\#S' \geq \#S$ and $v_1 := (2d+1, 0 \ldots, 0), \ldots, v_m := (0, \ldots, 0, 2d+1) \in S'$.*

Proof. For each i, we will either add v_i to S or replace one of the point in S with v_i to construct S'. So let $1 \leq i \leq m$. If $v_i \in S$, then we do not need to modify S. Assume now that $v_i \notin S$. If v_i is $2d$-separated from all the points in S, then we may take $S' = S \cup \{v_i\}$. Otherwise there is a point $s = (s_j) \in S$ such that $|s - v_i|_1 \leq 2d$. We will show that such s is unique, and so we may replace s with v_i to obtain S'. So suppose we have $t = (t_j) \in S$ with $|t - v_i|_1 \leq 2d$, and without loss of generality, assume $s_i \geq t_i$. Now

$$2d \geq |s - v_i|_1 = \sum_{j \neq i} s_j + 2d + 1 - s_i = 4d + 2 - 2s_i,$$

so $s_i \geq d+1$, and similarly, $t_i \geq d+1$. Hence

$$\begin{aligned}
|s - t|_1 &= s_i - t_i + \sum_{j \neq i} |s_j - t_j| \\
&\leq s_i - t_i + \sum_{j \neq i} s_j + \sum_{j \neq i} t_j \\
&\leq s_i - t_i + (2d + 1 - s_i) + (2d + 1 - t_i) \\
&= 4d + 2 - 2t_i \\
&\leq 2d.
\end{aligned}$$

Since S is $2d$-separated, this implies that $s = t$. Hence there is a unique point in $s \in S$ such that $|s - v_i|_1 \leq 2d$, and so if we take $S' := (S \setminus \{s\}) \cup \{v_i\}$, then S' will be $2d$-separated. □

We will call the v_i's the *corner points* since they are on the corners of the simplex $\Delta(m-1, 2d+1)$. We now consider the necessary and sufficient conditions for a point $s \in \Delta(m-1, 2d+1)$ to be $2d$-separated from all the corner points.

Lemma 1.4.4. *Let $d \geq 0$ and $m \geq 1$ be integers and $s = (s_j) \in \Delta(m-1, 2d+1) \subset \mathbb{Z}^m_{\geq 0}$. Then s is $2d$-separated from all the corner points if and only if $s_j \leq d$ for all $j = 1, \ldots, m$.*

Proof. First, note that if $s = (s_j) \in \Delta(m-1, 2d+1)$, then for all $i = 1, \ldots, m$,

$$|s - v_i|_1 = 2d + 1 - s_i + \sum_{j \neq i} s_j = 2d + 1 - 2s_i + \sum_{j=1}^{m} s_j = 2(d - s_i) + 2d + 2.$$

So s is $2d$-separated from v_i if and only if $2(d - s_i) + 2d + 2 > 2d$, which can be rearranged to

$$d + 1 > s_i.$$

Since d and s_i are integers, this inequality is equivalent to $d \geq s_i$. Hence s is $2d$-separated from all the corner points if and only if $d \geq s_i$ for all i. □

If we are constructing a maximum $2d$-separated set $S \subset \Delta(m-1, 2d+1)$, then by Lemma 1.4.3, we can assume that the set S contains all the corner points. Now consider the rest of the points $T := S \setminus \{v_1, \ldots, v_m\}$. For S to be $2d$-separated, T also needs to be $2d$-separated, and in addition, by Lemma 1.4.4, for all $t = (t_j) \in T$, we must have $t_j \leq d$ for all j. So in other words, Question 1.4.1 about the maximum size of S is equivalent to the following question. Also note that the sizes of the largest S in Question 1.4.1 and the largest T in the following question are related by $\#S = m + \#T$.

Question 1.4.5. Given m and d, how large can a set T be if it is $2d$-separated, contained in $\Delta(m-1, 2d+1)$, and for all $t = (t_i) \in T$, $t_i \leq d$ for all $i = 1, \ldots, m$.

The $d = 1$ case in Question 1.4.5 can be reformulated in terms of binary vectors as follows. Recall that a binary vector of length m is any vector in $\{0, 1\}^m$. The weight of such a vector is the sum of all the entries, and for two binary vectors v, v', the Hamming distance between v and v' is $|v - v'|_1$. Now if $d = 1$, then every entry in $t \in T$ is either 0 or 1, so we can consider t as a binary vector of length m. Moreover, since $t \in \Delta(m-1, 3)$, the weight of t is 3. In other words Question 1.4.5 for the $d = 1$ case is

asking for a largest set of binary vectors of length m with weight 3 that are pairwise Hamming distance being more than 2 apart.

The following theorem answers how large such a set of binary vectors can be. We state the theorem as in [Bro+90]. For the proof, see Theorem 3 in [Sch66]. Note that the Hamming distance between two binary vectors of the same weight must be even, so Hamming distance being more than 2 apart is equivalent to Hamming distance being at least 4 apart.

Theorem 1.4.6 (See Theorem 4, [Bro+90])**.** *Let $A(m, d, w)$ be the maximal possible number of binary vectors of length m, Hamming distance at least d apart and constant weight w. Then*

$$A(m,4,3) = \begin{cases} \lfloor \frac{m}{3} \lfloor \frac{m-1}{2} \rfloor \rfloor, & \text{if } m \not\equiv 5 \pmod 6 \\ \lfloor \frac{m}{3} \lfloor \frac{m-1}{2} \rfloor \rfloor - 1, & \text{if } m \equiv 5 \pmod 6 \end{cases}$$

So for all $m \geq 1$ and $d = 1$, the largest T in Question 1.4.5 has size $A(m, 4, 3)$, while the largest S in Question 1.4.1 has size $A(m, 4, 3) + m$, answering Question 1.4.5 and Question 1.4.1 respectively.

For small m's we can answer Question 1.4.2 fully.

Proposition 1.4.7. *Given $m = 1, 2$ or 3, the largest set S that is $2d$-separated and contained in $\Delta(m - 1, 2d + 1) \subset \mathbb{Z}^m_{\geq 0}$ has size $\#S = 1, 2$ and 4 respectively.*

Proof. By Lemma 1.4.3, we may assume that the corner points are already in S. Then for $m = 1$ and $m = 2$, there are no points in $\Delta(m - 1, 2d + 1)$ that are $2d$-separated from the corner points. So $\#S = m$ is the largest possible set.

For $m = 3$, suppose there exist 2 distinct points $s, s' \in \Delta(2, 2d + 1)$ that are $2d$-separated from the corner points. If $s = (a, b, c)$ and $s' = (a', b', c')$, then we have $0 \leq a, b, c, a', b', c' \leq d$ by Lemma 1.4.4. Since $|s|_1 = 2d + 1 = |s'|_1$, we may assume without loss of generality that $a \geq a'$, $b \leq b'$ and $c \leq c'$.

Then

$$\begin{aligned}|s - s'|_1 &= |a - a'| + |b - b'| + |c - c'| \\ &= a - a' + b' - b + c' - c \\ &= 2d + 1 - 2a' - (2d + 1) + 2a' \\ &= 2(a - a') \\ &\leq 2d\end{aligned}$$

so s and s' cannot be $2d$-separated. Hence S can only contain one more point apart from the corner point, and hence $\#S = 4$ is the largest. □

For other small m's, we can use a computer program to determine explicitly how large S can be for small d's. But we will first convert that question into a graph theory problem. Given $m \geq 1$ and $d \geq 0$ integers, let $G(m, d) := (V, E)$ be the graph with a vertex set V and an edge set E defined as follows: The vertices are points in $\Delta(m - 1, 2d + 1)$ with entries at most d, and an edge exists between distinct $s, s' \in V$ if

$$|s - s'|_1 = \sum_{i=1}^{m} |s_i - s'_i| \leq 2d.$$

Recall for a graph, an *independent set* is a set of vertices with no edges between them, and an independent set with the largest size is called a *maximum independent set*. The cardinality of such a maximum independent set is called the *independence number* of the graph. The set T in Question 1.4.5 is an independent set of $G(m, d)$, so we would like to know the independence number of $G(m, d)$ for a given $m \geq 1$ and $d \geq 0$.

Proposition 1.4.8. *For the following m and d, the size of the largest $2d$-separated set $S \subset \mathbb{Z}^m_{\geq 0}$ contained in $\Delta(m - 1, 2d + 1)$ is given in the table below.*

Table 1.2: Size of the largest $2d$-separated set $S \subset \mathbb{Z}_{\geq 0}^m$ contained in $\Delta(m-1, 2d+1)$

m \ d	1	2	3	4	5	6	7	8	9	10	11	12
4	5	6	6	7	7	7	7	7	8	8	8	8
5	7	10	10	10	11	11	12	12	12	13		
6	10	12	14	15								
7	14	18										
8	16	24										

Proof. As stated before the proposition, we would like to know the independence number of $G(m, d)$ to answer Question 1.4.5, and so we used the function `IndependenceNumber` in Magma[BCP97] to compute it. As noted in the paragraph before Question 1.4.5, the size of T in Question 1.4.5 is related to the size of S in Question 1.4.1 by $\#S = \#T + m$. So we added m to the output from `IndependenceNumber` to obtain the size of the largest set $S \subset \Delta(m-1, 2d+1)$ that is $2d$-separated, thus answering Question 1.4.1 completely for these values of m and d.

The missing entries in the table are due to the computations taking too long for those parameters. □

Remark 1.4.9. The independence number of a graph is a well known invariant and has been well studied. In particular, there are inequalities which involves the independence number and other invariants of a graph. See [Wil11, Chapter 3] for a list of such inequalities. Unfortunately the inequalities listed were either not strong enough, or had an invariant that was difficult to compute, and we could not obtain any useful bound for our graphs.

We would also like to note that the characteristic polynomial of the Laplacian matrix of $G(m, d)$ appear to have some pattern. In particular, one could predict most of the irreducible factors of the polynomial for $d = 1, 2$ and 3, including their multiplicities.

For any $m \geq 1$, we have the following construction of a suitable S.

Theorem 1.4.10. *Let $m \in \mathbb{Z}_+$. Then for any $d \geq m-1$, there exists a $2d$-separated set $S \subset \mathbb{Z}^m_{\geq 0}$ contained in $\Delta(m-1, 2d+1)$ with*

$$\#S = \begin{cases} \frac{m(m+2)}{4} & \text{if } m \text{ is even}, \\ \frac{(m+1)^2}{4} & \text{if } m \text{ is odd}. \end{cases}$$

Proof. We will explicitly construct such an S. For $1 \leq j \leq \frac{m}{2}$, $1 \leq k \leq m-2j$ and $r := \mathrm{ord}_2(j)$, let

$$v_{j,k} := (\underbrace{0, \ldots, 0}_{k-1}, d-r-k, \underbrace{0, \ldots, 0}_{j-1}, d, \underbrace{0 \ldots, 0}_{j-1}, r+k+1, \underbrace{0, \ldots, 0}_{m-2j-k}) \in \Delta(m-1, 2d+1).$$

To check that $v_{j,k} \in \Delta(m-1, 2d+1)$, we first verify that $d - r - k = d - \mathrm{ord}_2(j) - k \geq 0$.

$$\begin{aligned} d - \mathrm{ord}_2(j) - k &\geq d - \mathrm{ord}_2(j) - (m-2j) \\ &= d - m - \mathrm{ord}_2(j) + 2j \\ &\geq d - m + 2 \\ &\geq 0 \end{aligned}$$

where the last inequality follows from the assumption $d \geq m-1$. Looking at the length, we have $|v_{j,k}|_1 = d - r - k + d + r + k + 1 = 2d + 1$, so it has the correct length. Hence $v_{j,k}$ is a valid point in $\Delta(m-1, 2d+1)$.

We take

$$S := \{\text{corner points of } \Delta(m-1, 2d+1)\} \cup \left\{ v_{j,k} \;\middle|\; 1 \leq j \leq \tfrac{m}{2}, 1 \leq k \leq m-2j \right\}.$$

We first check if all the entries of $v_{j,k}$ are at most d to verify that they are $2d$-separated from the corner points. Since $d - r - k \leq d$, the only other value we need to check is $r + k + 1$, and

$$r + k + 1 = \mathrm{ord}_2(j) + k + 1 \leq \mathrm{ord}_2(j) + m - 2j + 1 \leq m - 2 + 1 = m - 1 \leq d.$$

Hence $v_{j,k}$ is $2d$-separated from the corner points.

Now we check that $v_{j,k}$'s are $2d$-separated. So fix two distinct $v_{j,k}$ and $v_{j',k'}$, and let

$$K := \{1 \leq i \leq m \mid (v_{j,k})_i \neq 0\} \quad \text{and} \quad K' := \{1 \leq i \leq m \mid (v_{j',k'})_i \neq 0\}$$

be the support of $v_{j,k}$ and $v_{j',k'}$ respectively. Note that $\#(K \cap K') \leq 2$, since $\#K = 3 = \#K'$ and $K = K'$ if and only if $v_{j,k} = v_{j',k'}$. Then

$$\begin{aligned} |v_{j,k} - v_{j',k'}|_1 &= \sum_{i \in K \cap K'} |(v_{j,k})_i - (v_{j',k'})_i| + \sum_{i \notin K \cap K'} (v_{j,k})_i + \sum_{i \notin K \cap K'} (v_{j',k'})_i \\ &\geq \sum_{i \notin K \cap K'} (v_{j,k})_i + \sum_{i \notin K \cap K'} (v_{j',k'})_i. \end{aligned}$$

Now suppose $\#(K \cap K') \leq 1$. Since the entries of $v_{j,k}$ are bounded by d, we have $\sum_{i \notin K \cap K'} (v_{j,k})_i \geq 2d + 1 - d = d + 1$, and similarly for $v_{j',k'}$. Hence

$$|v_{j,k} - v_{j',k'}|_1 \geq \sum_{i \notin K \cap K'} (v_{j,k})_i + \sum_{i \notin K \cap K'} (v_{j',k'})_i \geq (d+1) + (d+1) > 2d,$$

and so $v_{j,k}$ and $v_{j',k'}$ are $2d$-separated.

Now we consider the case when $\#(K \cap K') = 2$. There are three possible cases:

1. $j' = j$ and $k' = k + j$ (where the $k + j$-th position and the $k + 2j$-th position agree),
2. $j' = 2j$ and $k' = k$ (where the k-th position and the $k + 2j$-th position agree), or
3. $j' = 2j$ and $k' = k - j'$ (where the $k - 2j$-th position and the k-th position agree).

Note that if $j' \neq j$ and $j' \neq 2j$, then the spacing between the non-zero entries does not match, so the supports can only intersect at most 1 entry.

We first consider the case when $j' = j$ and $k' = k + j$. In this case, we have

$$
\begin{aligned}
&|v_{j,k} - v_{j,k'}|_1 \\
=&|(\underbrace{0, \ldots, 0}_{k-1}, d - r - k, \overbrace{0, \ldots, 0}^{k'-1}, r + k', \underbrace{0 \ldots, 0}_{j-1}, r + k + 1 - d, \underbrace{0, \ldots, 0}_{m-2j-k}, -r - k' - 1, \overbrace{0 \ldots, 0}^{m-2j-k'})|_1 \\
=&d - r - k + r + k' + d - (r + k + 1) + r + k' + 1 \\
=&2d + 2k' - 2k \\
>&2d
\end{aligned}
$$

so they are $2d$-separated.

If $j' = 2j$ and $k' = k$ then we have

$$
\begin{aligned}
&|v_{j,k} - v_{j',k'}|_1 \\
=&|(\underbrace{0, \ldots, 0}_{k-1}, -r + r', \overbrace{0, \ldots, 0}^{j'-1}, d, \underbrace{0 \ldots, 0}_{j-1}, r + k + 1 - d, \underbrace{0, \ldots, 0}_{m-2j-k}, r' + k' + 1, \overbrace{0, \ldots, 0}^{m-2j'-k'})|_1 \\
=&-r + r' + d + d - (r + k + 1) + r' + k' + 1 \\
=&2d + 2(r' - r) \\
=&2d + 2(\mathrm{ord}_2(2j) - \mathrm{ord}_2(j)) \\
>&2d
\end{aligned}
$$

so these points are $2d$-separated.

Finally if $j' = 2j$ and $k' = k - j'$, then we have

$$\begin{aligned}
&|v_{j,k} - v_{j',k'}|_1 \\
=&|(\underbrace{\overbrace{0,\ldots,0}^{k'-1}, d - r' - k', \overbrace{0,\ldots,0}^{j'-1}}_{k-1}, -r - k, \overbrace{\underbrace{0,\ldots,0}_{j-1}, d, \underbrace{0,\ldots,0}_{j-1}}^{j'-1}, r + k - r' - k', \overbrace{\underbrace{0,\ldots,0}_{m-2j-k}}^{m-2j'-k'})|_1 \\
=&d - r' - k' + r + k + d + r + k - r' - k' \\
=&2d + 2(k - k') + 2(r - r') \\
>&2d,
\end{aligned}$$

and those points are also $2d$-separated.

Finally we count how many points we get from this construction. If m is even, this gives total of

$$m + \sum_{j=1}^{m/2} (m - 2j) = \frac{m(m+2)}{4}$$

points, and if m is odd,

$$m + \sum_{j=1}^{(m-1)/2} (m - 2j) = \frac{(m+1)^2}{4}$$

points. □

Remark 1.4.11. One could add more points to the set S given in Theorem 1.4.10 by considering points with larger support. If a point has a support of size 5 and has all its non-zero entries taking values around $\frac{2d+1}{5}$, then it will be $2d$-separated from any points in S. More generally, if u' is the size of the support of the previous point added, then one could add a point with support of size $u > 2u'$ with all its non-zero entries taking values around $\frac{2d+1}{u}$. While this does increase the size of S, it is only useful for large m, and it does not appear to increase the asymptotic of the size of S.

We conclude the section with an upper bound on the size of a $2d$-separated set S contained in $\Delta(m-1, 2d+1)$. We will first give an equivalent formulation of Question 1.4.2 by putting all the d's together that will be useful for proving the upper bound.

Question 1.4.12. Let $m \in \mathbb{Z}_+$. Consider the regular $(m-1)$-simplex

$$\Delta_{m-1} := \left\{ v \in \mathbb{R}^m \;\middle|\; v_i \geq 0, \sum_{i=1}^{m} v_i = 1 \right\}.$$

What is the maximum $S \subset \Delta_{m-1}$ that is 1-separated?

Remark 1.4.13. We can convert between the S's in Question 1.4.2 and Question 1.4.12 in the following way. If a set $S \subset \Delta(m-1, 2d+1)$ is $2d$-separated, then $S' := \left\{ \frac{1}{2d+1} s \;\middle|\; s \in S \right\} \subset \mathbb{Q}^m_{\geq 0}$ is contained in Δ_{m-1}. Now if $s, t \in S$ are distinct points, then $|s-t|_1 > 2d$. But since $|s|_1 = |t|_1$ and $s, t \in \mathbb{Z}^m_{\geq 0}$, the distance $|s-t|_1$ must be even, so $|s-t|_1 \geq 2d+2$. Hence S' is 1-separated and satisfies the conditions in Question 1.4.12.

On the other hand, suppose $S \subset \Delta_{m-1}$ is 1-separated. For each $s \in S$, take a nearby point $s' := (s'_i) \in \Delta_{m-1} \cap \mathbb{Q}^m$ such that the denominators of the s'_i's are odd. Let S' be the set of all these s''s. Since being 1-separated is an open condition, if we take s' to be close enough to s, then S' will be 1-separated. Now suppose $2d+1$ is the LCM of the denominators appearing in the entries of all $s' \in S'$. Then $S'' := \{(2d+1)s' \mid s' \in S'\} \subset \mathbb{Z}^m_{\geq 0}$ is contained in $\Delta(m-1, 2d+1)$ and is $2d$-separated. Hence S'' satisfies the conditions in Question 1.4.2.

Proposition 1.4.14. *Let $m \in \mathbb{Z}_+$. Then for any $S \subset \Delta_{m-1}$ that is 1-separated, we have*

$$\#S \leq 4^{m-1}.$$

Proof. Suppose we have such an S. Then around each point $s \in S$, we have a radius $\frac{1}{2}$ (in ℓ_1-norm) ball $B(s, \frac{1}{2})$ such that none of these balls intersect each other. So we have

$$\sum_{s \in S} \operatorname{vol}\left(B(s, \tfrac{1}{2}) \cap \Delta_{m-1}\right) \leq \operatorname{vol}(\Delta_{m-1}).$$

The volume of $B(s, \frac{1}{2}) \cap \Delta_{m-1}$ is the smallest when s is a corner point of Δ_{m-1} since Δ_{m-1} is a convex polytope. For a corner point $v_1 := (1, 0, \ldots, 0)$,

$$B(v_1, \tfrac{1}{2}) \cap \Delta_{m-1} = \left\{ (u_i) \in \mathbb{R}^m \;\middle|\; \frac{3}{4} \leq u_1 \leq 1, 0 \leq u_i \leq \frac{1}{4} \; \forall \; 2 \leq i \leq m, \sum_{i=1}^{m} u_i = 1 \right\},$$

which is a $(m-1)$-simplex with vertices $(1, 0, \ldots, 0), (\frac{3}{4}, \frac{1}{4}, 0, \ldots, 0), \ldots, (\frac{3}{4}, 0, \ldots, 0, \frac{1}{4})$. This simplex has side lengths $\frac{1}{4}$ of the side lengths of the simplex Δ_{m-1}, so

$$\#S \left(\tfrac{1}{4}\right)^{m-1} \operatorname{vol}(\Delta_{m-1}) \leq \sum_{s \in S} \operatorname{vol}\left(B(s, \tfrac{1}{2}) \cap \Delta_{m-1}\right) \leq \operatorname{vol}(\Delta_{m-1}).$$

Hence $\#S \leq 4^{m-1}$. □

We can translate the upper bound for Question 1.4.12 to an upper bound for Question 1.4.2.

Corollary 1.4.15. *Let $m \geq 1$ be an integer. Suppose $S \subset \Delta(m-1, 2d+1) \subset \mathbb{Z}^m_{\geq 0}$ is a $2d$-separated set for some $d \geq 0$. Then $\#S \leq 4^{m-1}$.*

Proof. By Remark 1.4.13, any set $S \subset \Delta(m-1, 2d+1)$ that is $2d$-separated can be converted to a set $S' \subset \Delta_{m-1}$ that is 1-separated. By Proposition 1.4.14, $\#S' \leq 4^{m-1}$, so $\#S = \#S' \leq 4^{m-1}$. □

1.5 A Ring with Trace Zero Non-commutators of Arbitrary Large Size

In this section, we construct a Noetherian domain Λ of dimension 1 that admits an $n \times n$ trace 0 non-commutator matrix over Λ for all $n \geq 2$. We use the following theorem of Heinzer and Levy to construct the ring, and then apply Corollary 1.3.4 with varying maximal ideals to show that there is a trace 0 non-commutator of arbitrary size.

Theorem 1.5.1 (Theorem 2.1 [HL07]). *Let K be a field and I a nonempty set. For each $i \in I$, let $(\Lambda_i, \mathfrak{n}(i))$ be a Noetherian local integral domain of dimension 1 with maximal ideal $\mathfrak{n}(i)$ such that Λ_i is a subring of K and the quotient field $Q(\Lambda_i)$ equals K. Suppose:*

1. *Every non-zero element of K is a unit in all but finitely many Λ_i; and*
2. *For every pair of distinct indices $j \neq h$ there exist elements $x_j \in \Lambda_j$ and $x_h \in \Lambda_h$ such that:*
   (a) *x_j and x_h are non-units in Λ_j and Λ_h respectively;*
   (b) *x_j is a unit in Λ_i when $i \neq j$, and x_h is a unit in Λ_i when $i \neq h$;*
   (c) *$x_j + x_h$ is a unit in Λ_i for every i.*

Then the ring $\Lambda := \bigcap_i \Lambda_i$ is Noetherian of dimension 1, its distinct maximal ideals are $\mathfrak{m}(i) := \mathfrak{n}(i) \cap \Lambda$, and $\Lambda_i = \Lambda_{\mathfrak{m}(i)}$ for each $i \in I$.

Theorem 1.5.2. *There exists a Noetherian commutative domain Λ with dimension 1 such that for every $n \geq 2$, there exists a trace 0 non-commutator in $\mathrm{M}_n(\Lambda)$.*

Proof. We will start with the construction of the field K needed to apply Theorem 1.5.1. Let k be an algebraically closed field and $S := k[X_{ij} : i \geq 2, 1 \leq j \leq i]$, a polynomial ring with infinitely many variables. Let $J \subset S$ be the ideal generated by the following elements:

$$J := (X_{i1}^2 - X_{ij}^{p_j} : i \geq 2, 2 \leq j \leq i),$$

where p_j is the j-th prime.

Claim 1. $R := S/J$ is an integral domain.

Proof of Claim 1. We show that R is an integral domain by proving that J is a prime ideal. So let $g, h \in S$ be such that $gh \in J$. Then

$$gh = \sum_{i \geq 2} \sum_{j=2}^{i} a_{ij}(X_{i1}^2 - X_{ij}^{p_j}),$$

for some $a_{ij} \in S$ with only finitely many of the a_{ij}'s being non-zero. Then there are only finitely many variables X_{ij} appearing in the equation, so we may restrict our ring S to

$$S_n := k[X_{ij} : 2 \leq i \leq n, 2 \leq j \leq i],$$

and the ideal J to an ideal

$$J_n := (X_{i1}^2 - X_{ij}^{p_j} : 2 \leq i \leq n, 2 \leq j \leq i) \subset S_n,$$

for some n. Then $g \in J_n$ or $h \in J_n$ will imply $g \in J$ or $h \in J$, so it is sufficient to show that J_n is a prime ideal. We will prove that S_n/J_n is a domain in order to show that J_n is a prime ideal. Now,

$$S_n/J_n \cong k[X_{21}, X_{22}]/(X_{21}^2 - X_{22}^3) \underset{k}{\otimes} \ldots \underset{k}{\otimes} k[X_{n1}, \ldots, X_{nn}]/(X_{n1}^2 - X_{n2}^3, \ldots, X_{n1}^2 - X_{nn}^{p_n}).$$

A tensor product of finitely generated k-algebras that are domains is a domain if k is algebraically closed (see proof of [Stacks, Tag 05P3]). So if

$$T_t := k[X_1, \ldots, X_t]/(X_1^2 - X_2^3, \ldots, X_1^2 - X_t^{p_t}),$$

is a domain for all $2 \leq t \leq n$, then S_n/J_n is also a domain.

Now we will prove that T_t is a domain by induction on t, along with the fact that $[Q(T_t) : k(X_1)] = p_2 p_3 \cdots p_t$ where $Q(T_t)$ is the quotient field of T_t. If $t = 2$, then $T_2 = k[X_1, X_2]/(X_1^2 - X_2^3)$. Now

$X_1^2 - X_2^3$ is an irreducible polynomial in $k[X_1, X_2]$, and $k[X_1, X_2]$ is a UFD, so $X_1^2 - X_2^3$ is a prime element. Hence T_2 is a domain, and $[Q(T_2) : k(X_1)] = 3$. Now suppose that T_{t-1} is a domain and $[Q(T_{t-1}) : k(X_1)] = p_2 p_3 \cdots p_{t-1}$. Since

$$T_t \cong T_{t-1}[X_t]/(X_t^{p_t} - X_1^2),$$

we only need to show that $f_t := X_t^{p_t} - X_1^2$ is prime in $T_{t-1}[X_t]$ to show that T_t is a domain. We first show that f_t is irreducible in $k(X_1)[X_t]$. Now $f_t = X_t^{p_t} - X_1^2$ has a prime degree and $k(X_1)$ contains all the p_t-th roots of unity, so by [Lano2, Theorem VI.9.1], f_t is irreducible in $k(X_1)[X_t]$ if and only if it has no roots in $k(X_1)$. It is clear that f_t has no roots in $k(X_1)$, so f_t is irreducible in $k(X_1)[X_t]$. Now $\deg f_t = p_t$ is a prime and does not divide $[Q(T_{t-1}) : k(X_1)] = p_2 p_3 \cdots p_{t-1}$, so f_t is still irreducible in $Q(T_{t-1})[X_t]$. Hence f_t is a prime in $Q(T_{t-1})[X_t]$ since $Q(T_{t-1})[X_t]$ is a UFD.

Now will use the fact that f_t is a prime in $Q(T_{t-1})[X_t]$ to show that f_t is a prime in $T_{t-1}[X_t]$. So suppose $f_t \mid gh$ for some $g, h \in T_{t-1}[X_t]$. Since f_t is a prime in $Q(T_{t-1})[X_t]$, we may assume that $f_t g' = g$ for some $g' := \sum_{i=0}^{n'} g_i' X_t^i \in Q(T_{t-1})[X_t]$ without loss of generality. Suppose $g' \notin T_{t-1}[X_t]$. Then there exists a maximal index j such that $g_j' \notin T_{t-1}$. If $g = \sum_{i=0}^{n} g_i X_t^i$, then looking at the degree $j + p_t$ coefficients of the equation $f_t g' = g$, we have

$$g_{j+p_t} = g_j' - g_{j+p_t}' X_1^2.$$

We have $g_{j+p_t}' \in T_{t-1}$ since j was the maximal index such that $g_j' \notin T_{t-1}$. Hence $g_j' = g_{j+p_t} + g_{j+p_t}' \in T_{t-1}$, which is a contradiction, so $g' \in T_{t-1}[X_t]$. Hence we have $f_t \mid g$ in $T_{t-1}[X_t]$ and so f_t is a prime in $T_{t-1}[X_t]$. This implies that $T_t = T_{t-1}[X_t]/(f_t)$ is a domain, and now $Q(T_t) = Q(T_{t-1})[X_t]/(f_t)$, so

$$[Q(T_t) : k(X_1)] = [Q(T_t) : Q(T_{t-1})][Q(T_{t-1}) : k(X_1)] = p_t p_2 p_3 \cdots p_{t-1},$$

and we are done. Hence T_t, S_n/J_n and $R = S/J$ are all domains and we have proved Claim 1. $\square$

Since R is a domain, we may take $K := Q(R)$, the quotient field of R. This will be the K we take for applying Theorem 1.5.1. We now define the Λ_n's needed to apply Theorem 1.5.1. We take the set I to be $\mathbb{N}$. Let $Y_{ij} \in R \subset K$ be the residue class of X_{ij}. For $n \geq 2$, define a subfield

$$F_n := k(Y_{ij} : i \neq n, 1 \leq j \leq i) \subset K,$$

and a subring

$$R_n := F_n[Y_{n,1}, \ldots, Y_{n,n}] \subset K.$$

Let $P_n := F_n[Z_1, \ldots, Z_n]$ be the polynomial ring in n variables.

Claim 2.

$$\begin{aligned} \varphi_n : P_n/(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}) &\longrightarrow R_n = F_n[Y_{n,1}, \ldots, Y_{n,n}] \\ \overline{Z}_i &\longmapsto Y_i, \end{aligned}$$

is an isomorphism, where $\overline{Z}_i$ is the residue class of Z_i.

Proof of Claim 2. It is clear that φ_n is surjective, so let us show that it is injective. Consider the lift of φ_n,

$$\begin{aligned} \tilde{\varphi}_n : P_n &\longrightarrow R_n = F_n[Y_{n,1}, \ldots, Y_{n,n}] \\ Z_i &\longmapsto Y_i. \end{aligned}$$

We see that $\ker \tilde{\varphi}_n \supset (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n})$, so to conclude that φ_n is injective, we only need to show that

$$\ker \tilde{\varphi}_n \subset (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}).$$

So suppose that $f \in \ker \tilde{\varphi}_n$. If $c \in F_n^\times$ is the product of the denominators of the coefficients of f, then

$$cf \in k[Y_{ij} : i \neq n, 1 \leq j \leq i][Z_1, \ldots, Z_n] =: P_n' \subset P_n.$$

Moreover, $cf \in (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n})$ implies $f \in (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n})$, so it is sufficient to check that

$$\ker\left(\tilde{\varphi}_n|_{P_n'}\right) \subset (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n})P_n' \subset P_n'.$$

We have the following commutative diagram

$$\begin{array}{ccc} S = k[X_{ij} : i \geq 2, 1 \leq j \leq i] & & \\ \downarrow{\scriptstyle \psi_n} & \overset{q}{\searrow} & \\ P_n' = k[Y_{ij} : i \neq n, 1 \leq j \leq i][Z_1, \ldots, Z_n] & \xrightarrow{\tilde{\varphi}_n|_{P_n'}} & \tilde{\varphi}_n(P_n') = k[Y_{ij} : i \geq 2, 1 \leq j \leq i] = S/J \end{array},$$

where q is the quotient map and

$$\begin{aligned} \psi_n : S &\longrightarrow P_n' \\ X_{ij} &\longmapsto \begin{cases} Y_{ij} & \text{if } i \neq n, \\ Z_j & \text{if } i = n. \end{cases} \end{aligned}$$

Since ψ_n is surjective, $\ker \tilde{\varphi}_n|_{P_n'} = \psi_n(\ker q) = \psi_n(J)$, and

$$\psi_n(J) = (\psi_n(X_{i1})^2 - \psi_n(X_{ij})^{p_j} : i \geq 2, 2 \leq j \leq i) = (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}) \subset P_n'.$$

Hence

$$\ker \tilde{\varphi}_n|_{P_n'} = (Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}) \subset P_n',$$

and φ_n is an isomorphism. □

Since $P_n/(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n})$ is easier to work with than R_n, we will use the former presentation to prove properties about R_n to verify the assumptions of Theorem 1.5.1.

The ideal $(Y_{n,1}, \ldots, Y_{n,n}) \subset R_n$ is maximal since it corresponds to $(\overline{Z}_1, \ldots, \overline{Z}_n)$ so we may localise R_n at $(Y_{n,1}, \ldots, Y_{n,n})$ to obtain a local domain

$$\Lambda_n := (R_n)_{(Y_{n,1},\ldots,Y_{n,n})} \subset K,$$

with a maximal ideal $\mathfrak{n}(n) := (Y_{n,1}, \ldots, Y_{n,n}) \subset \Lambda_n$. Since Λ_n is a localisation of a finitely generated F_n-algebra, it is Noetherian.

Now we show that $\dim \Lambda_n = 1$. We have an isomorphism

$$\Lambda_n \cong \left(P_n/(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n})\right)_{(\overline{Z}_1,\ldots,\overline{Z}_n)},$$

through φ_n. We may interchange localisation and quotient so

$$\Lambda_n \cong (P_n)_{(Z_1,\ldots,Z_n)}/(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}),$$

as well. Now

$$\left(Z_1, Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}\right) = \left(Z_1, Z_2^3, \ldots, Z_n^{p_n}\right) \subset (P_n)_{(Z_1,\ldots,Z_n)}$$

is a $(Z_1, \ldots, Z_n)$-primary ideal, so $Z_1, Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}$ is a system of parameters of $(P_n)_{(Z_1,\ldots,Z_n)}$ (see the start of [Mat89, Ch. 14] for the definition of a system of parameters). Hence by [Mat89, Theorem 14.1],

$$\dim \Lambda_n = \dim (P_n)_{(Z_1,\ldots,Z_n)}/(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_n^{p_n}) = n - (n-1) = 1.$$

Finally note that Λ_n contains all Y_{ij}'s, so $R \subset \Lambda_n \subset K = Q(R)$. Hence to apply Theorem 1.5.1, we only need to verify conditions (1) and (2).

For (1), if $f \in K$, then f can be written as a rational function in the Y_{ij}'s. If f is non-zero, then only finitely many Y_{ij}'s appear in such a representation of f. If $n \geq 2$ is such that Y_{nj} does not appear in such

a representation for all $1 \leq j \leq n$, then $f \in F_n$, so $f \in \Lambda_n$ is a unit. Hence any non-zero element in K is a unit in all but finitely many Λ_n's.

For (2), if $j \neq h$, then take $x_j := Y_{j,1}$ and $x_h := Y_{h,1}$. These are not units in Λ_j and Λ_h respectively, and are units in Λ_i for other i's not equal to j or h. Moreover, if $i \neq j$ and $i \neq h$, then $x_j + x_h \in F_i \subset R_i$ so $x_j + x_h$ is a unit in Λ_i. Hence $\Lambda := \bigcap_i \Lambda_i$ is a Noetherian domain of dimension 1 by Theorem 1.5.1.

Finally, we show that the embedding dimension of $\mathfrak{m}(i) := \mathfrak{n}(i) \cap \Lambda$ is i. This will prove the theorem since for all $n \geq 2$, we can find i such that $n \leq \frac{i+1}{2}$, and we can apply Corollary 1.3.4 with $R = \Lambda$ and $\mathfrak{m} = \mathfrak{m}(i)$ to construct an $n \times n$ trace 0 non-commutator.

We now compute the embedding dimension of $\mathfrak{m}(i)$'s. Since $\Lambda_i = \Lambda_{\mathfrak{m}(i)}$ by Theorem 1.5.1, we can check the embedding dimension of the local ring Λ_i instead. We have

$$\Lambda_i \cong (P_i)_{(Z_1,\ldots,Z_i)}/(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_i^{p_i}),$$

so

$$\mathfrak{n}(i)/\mathfrak{n}(i)^2 \cong (\overline{Z}_1, \ldots, \overline{Z}_i)/(\overline{Z}_1, \ldots, \overline{Z}_i)^2.$$

Now we show that $\overline{Z}_1, \ldots, \overline{Z}_i$ form an F_i-basis of $(\overline{Z}_1, \ldots, \overline{Z}_i)/(\overline{Z}_1, \ldots, \overline{Z}_i)^2$. So suppose

$$a_1\overline{Z}_1 + \cdots + a_i\overline{Z}_i \in (\overline{Z}_1, \ldots, \overline{Z}_i)^2, \tag{1.2}$$

for some $a_1, \ldots, a_i \in F_i$. Now

$$(Z_1^2 - Z_2^3, \ldots, Z_1^2 - Z_i^{p_i}) \subset (Z_1, \ldots, Z_i)^2,$$

so we can lift eq. (1.2) to $(P_i)_{(Z_1,\ldots,Z_n)}$ to obtain

$$a_1Z_1 + \cdots + a_iZ_i \in (Z_1, \ldots, Z_i)^2.$$

But then $a_j = 0$ for all j since all the terms in the left-hand side are degree 1. Hence

$$\dim_{F_i}(\overline{Z}_1, \ldots, \overline{Z}_i)/(\overline{Z}_1, \ldots, \overline{Z}_i)^2 = i$$

□

1.6 Trace Zero 2×2 Matrices

In this section, we summarise the current progress on the case of 2×2 matrices. We start by recalling various facts and definitions needed to state Theorem 1.6.14 where we put together known results from the 1970s and 1980s. We then review facts and definitions on the K-theory of affine surfaces to be able to state more recent results such as Theorem 1.6.23,Corollary 1.6.25 and Theorem 1.6.27.

For this section, we assume that $\mathrm{Spec}(R)$ is connected for any ring R. This is not a strong assumption since we can always reduce the question about commutators to the case where $\mathrm{Spec}(R)$ is connected if R is Noetherian. Indeed, if R is a Noetherian ring, then $\mathrm{Spec}(R)$ has only finitely many connected components, and $R = \prod_{i=1}^{r} R_i$ where $\mathrm{Spec}(R_i)$ is a connected component of $\mathrm{Spec}(R)$. A matrix $M \in \mathrm{M}_n(\prod_{i=1}^{r} R_i)$ is a commutator if and only if all M_i's are commutators where $M = (M_i) \in \prod_{i=1}^{r} \mathrm{M}_n(R_i) \cong \mathrm{M}_n(\prod_{i=1}^{r})$.

Lissner showed by elementary means that $\begin{pmatrix} c_1 & c_2 \\ c_3 & -c_1 \end{pmatrix} \in \mathrm{M}_2(R)$ is a commutator except possibly when $c_i \notin (c_j, c_k) \subset R$ for any $(i\ j\ k)$ which is a permutation of $(1\ 2\ 3)$ (see [Lis61, Lemma 3.1 and 3.3]).

The main tool in the 2×2 case is the following lemma connecting a commutator with an exterior power. Recall that $v \in \wedge^p R^n$ is *decomposable* if there exist $v_1, \ldots, v_p \in R^n$ such that $v = v_1 \wedge \cdots \wedge v_p$.

Lemma 1.6.1. *Let* $M := \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathrm{M}_2(R)$. *Then* M *is a commutator if and only if* $ae_2 \wedge e_3 + be_3 \wedge e_1 + ce_1 \wedge e_2 \in \wedge^2 R^3$ *is decomposable. In particular, every* 2×2 *trace* 0 *matrix is a commutator if and only if every vector in* $\wedge^2 R^3$ *is decomposable.*

Proof. Suppose $M = [X_1, X_2]$ for some $X_1, X_2 \in \mathrm{M}_2(R)$. Then $M = [X_1 + rI_2, X_2 + sI_2]$ for any $r, s \in R$, so we may assume that $X_i = \begin{pmatrix} x_i & z_i \\ y_i & 0 \end{pmatrix}$ for some $x_i, y_i, z_i \in R$ for $i = 1, 2$. Then the equation $M = [X_1, X_2]$ becomes

$$a = y_2 z_1 - z_2 y_1$$

$$b = z_2 x_1 - x_2 z_1$$

$$c = x_2 y_1 - y_2 x_1$$

which is equivalent to

$$ae_2 \wedge e_3 + be_3 \wedge e_1 + ce_1 \wedge e_2 = (x_2 e_1 + y_2 e_2 + z_2 e_3) \wedge (x_1 e_1 + y_1 e_2 + z_1 e_3).$$

Hence M being a commutator is equivalent to the vector being decomposable.

Since $e_2 \wedge e_3, e_3 \wedge e_1, e_1 \wedge e_2$ form a basis for $\wedge^2 R^3$, there is a bijection between 2×2 trace 0 matrices and $\wedge^2 R^3$. Hence all the trace 0 matrices being a commutator is equivalent to all the vectors in $\wedge^2 R^3$ being decomposable. □

Definition 1.6.2. Given $n \geq 1$, we say that R *is* T_n^{n+1} if every vector in $\wedge^n R^{n+1}$ is decomposable. We call a ring R an *OP-ring* if it is T_n^{n+1} for all $n \geq 1$.

This definition was made by David Lissner in [Lis65] and OP stands for *outer product*.

Remark 1.6.3. Lemma 1.6.1 can be rephrased as stating that every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator if and only if R is T_2^3.

From here on in this section, we will focus on the case when R is Noetherian. For non-Noetherian OP rings, see [JW17].

Given a property P, we say that a ring R is *locally P* if every localisation of R at a prime ideal has the property P. For T_n^{n+1} or OP, locally true at every prime is equivalent to locally true at every maximal ideal.

Proposition 1.6.4. *A Noetherian ring R is locally T_n^{n+1} or locally OP if and only if every localisation of R at a maximal ideal is T_n^{n+1} or OP, respectively.*

Proof. If R is locally T_n^{n+1}, then every localisation of R at a maximal ideal is T_n^{n+1} by definition. On the other hand, suppose every localisation of R at a maximal ideal is T_n^{n+1}, and let $\mathfrak{p} \subset R$ be a prime ideal. Then there exists a maximal ideal $\mathfrak{m} \supset \mathfrak{p}$, and $R_\mathfrak{p}$ is a localisation of $R_\mathfrak{m}$ at $\mathfrak{p}R_\mathfrak{m}$. Now let $u \in \wedge^n R_\mathfrak{p}^{n+1}$. Then there exists $r \in R_\mathfrak{m} \setminus \mathfrak{p}R_\mathfrak{m}$ such that $ru \in \wedge^n R_\mathfrak{m}^{n+1}$. Since $R_\mathfrak{m}$ is T_n^{n+1}, ru is decomposable, so

$$ru = v_1 \wedge \cdots \wedge v_n$$

for some $v_1, \ldots, v_n \in R_\mathfrak{m}^{n+1}$. Now

$$u = \tfrac{1}{r} v_1 \wedge \cdots \wedge v_n \in \wedge^n R_\mathfrak{p}^{n+1}$$

so u is decomposable. Hence $R_\mathfrak{p}$ is T_n^{n+1}. The equivalence for OP follows from the equivalence for T_n^{n+1} for all $n \geq 1$. □

For a local ring, the OP property can be detected by the minimal number of generators for its maximal ideal.

Theorem 1.6.5 (Theorem [Tow70])**.** *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then R is an OP-ring if and only if $\mathfrak{m}$ is generated by 2 elements.*

Corollary 1.6.6. *Let R be a regular ring of dimension $d \leq 2$. Then R is locally OP.*

Proof. Let $\mathfrak{m} \subset R$ be a maximal ideal. Then $R_\mathfrak{m}$ is a regular local ring of dimension $\leq d$, so $\mathfrak{m}R_\mathfrak{m}$ is generated by at most 2 elements. Hence $R_\mathfrak{m}$ is an OP ring by Theorem 1.6.5, and so R is locally OP. □

Recall that a *semilocal ring* is a ring with finitely many maximal ideals. For semilocal rings, the OP property can be detected locally.

Theorem 1.6.7 (Theorem [Hin72]). *Let R be a Noetherian semilocal ring. Then R is an OP-ring if and only if R is locally OP.*

Lissner first used the term OP-ring in [Lis65] and showed that a Dedekind domain is an OP-ring in [Lis65, Appendix]. Towber subsequently showed that if R is a Dedekind domain then $R[x]$ is an OP-ring in [Tow68, Theorem 1.2]. Estes and Matijevic then proved the following characterisation of OP-rings. Recall that an R-module M is *R-oriented* if $\wedge^n M \cong R$ for some $n \geq 1$.

Theorem 1.6.8 (Theorem 1, Corollary 1, Corollary 2 [EM80]). *Let R be a Noetherian ring satisfying one of the following properties:*

- *R is reduced,*
- *every minimal ideal of R is principal, or*
- *R has only finitely many maximal ideals with non-regular localisation.*

Then R is an OP-ring if and only if R is locally OP and every finitely generated R-oriented module is free.

Remark 1.6.9. Estes and Matijevic note in [EM80, Page 1356] that the three conditions on R are probably not necessary, and suspects that every R-oriented module being free and R being locally OP are the only necessary conditions for R to be an OP-ring.

Corollary 1.6.10. *Let R be a reduced Noetherian locally OP ring. Then any finitely generated R-oriented module is projective.*

Proof. Let M be a finitely generated R-oriented module, so that $\wedge^n M = R$ for some $n \geq 1$. We will show that M is projective by showing that it is locally free. So let $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime ideal. Then

$$R_{\mathfrak{p}} = (\wedge^n M) \underset{R}{\otimes} R_{\mathfrak{p}} = \wedge^n M_{\mathfrak{p}}.$$

Now R is locally OP and so $R_{\mathfrak{p}}$ is an OP-ring, and $M_{\mathfrak{p}}$ is a finitely generated $R_{\mathfrak{p}}$-oriented module, so $M_{\mathfrak{p}}$ is free by Theorem 1.6.8. Hence M is projective. □

Recall that an R-module M is *stably-free* if $M \oplus R^m \cong R^n$ for some n and m.

Lemma 1.6.11 ((3) Lemma, (4) Lemma in [BDG80]). *Let R be a Noetherian T_2^3 ring. Then every maximal ideal of R is generated by two elements and every finitely generated stably-free projective R-module is free.*

Recall that the *Grothendieck group* of a ring R, $K_0(R)$, is the group completion of the monoid of isomorphism classes of finitely generated projective R-modules, under direct sum. And $SK_0(R)$ is the subgroup of $K_0(R)$ consisting of the classes $[P] - [R^m]$, where P is an R-oriented projective module of constant rank m (cf. [Wei13, Definition II.2.6.1]).

Lemma 1.6.12 ((5) Proposition [BDG80]). *Let R be a dimension 2 Noetherian ring, and suppose that every maximal ideal of R of height 2 is generated by 2 elements. Then $SK_0(R) = 0$.*

Lemma 1.6.13 ((6) Lemma [BDG80]). *Let R be a Noetherian ring and suppose that $SK_0(R) = 0$. Then every finitely generated stably-free projective R-module is free if and only if every finitely generated R-oriented projective R-module is free.*

We combine the works of Estes–Matijevic [EM80] and Boratyński–Davis–Geramita [BDG80] to obtain the following theorem.

Theorem 1.6.14. *Let R be a Noetherian ring satisfying one of the following conditions:*

- *R is reduced,*
- *every minimal ideal of R is principal, or*
- *R has only finitely many maximal ideals with non-regular localisation.*

Then the following are equivalent:

1. *Every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator,*
2. *R is T_2^3,*
3. *R is an OP-ring,*

4. *R is locally OP and every finitely generated projective R-oriented module is free,*

5. *R is locally OP, $SK_0(R) = 0$ and every finitely generated stably-free projective R-module is free, and*

6. *Every maximal ideal of R is generated by two elements and every finitely generated stably-free projective R-module is free.*

Proof. (1) is equivalent to (2) by Lemma 1.6.1. (3) implies (2) follows from the definition of an OP-ring. (4) implies (3) is Theorem 1.6.8 with Corollary 1.6.10.

For (5) implies (4), suppose M is an R-oriented module. Then for all prime ideal $\mathfrak{p}$, $M_\mathfrak{p}$ is $R_\mathfrak{p}$-oriented module, and since $R_\mathfrak{p}$ is OP, every $R_\mathfrak{p}$-oriented module is free. Hence M is an R-oriented projective module. Hence it is stably-free projective by Lemma 1.6.13 and hence free by (5).

For (6) implies (5), if every maximal ideal of R is generated by 2 elements, then every maximal ideal is locally generated by at most two elements. Hence every localisation is OP by Theorem 1.6.5. Now for all maximal ideal $\mathfrak{m}$, $\mathfrak{m}R_\mathfrak{m}$ is generated by at most 2 elements, so $\dim R_\mathfrak{m} \leq 2$ by Krull's Height theorem [Mat89, Theorem 13.5]. Hence $\dim R \leq 2$, and so by Lemma 1.6.12, $SK_0(R) = 0$.

(2) implies (6) is Lemma 1.6.11. □

Corollary 1.6.15. *Let R be a locally OP Noetherian ring. Then*

1. $\dim R \leq 2$,

2. *If* $\dim R = 0$ *then R is an OP-ring,*

3. *If* $\dim R = 1$ *and if R satisfies one of the following, then R is an OP-ring.*

   (a) *R is reduced,*

   (b) *every minimal ideal of R is principal, or*

   (c) *R has only finitely many maximal ideals with non-regular localisation.*

Proof. If R is locally OP Noetherian ring, then by Theorem 1.6.5, $\mathfrak{m}R_{\mathfrak{m}}$ is generated by 2 elements for any maximal ideal $\mathfrak{m}$ of R. Hence $\dim R_{\mathfrak{m}} \leq 2$ by Krull's Height theorem [Mat89, Theorem 13.5], and so $\dim R \leq 2$.

(2) follows from Theorem 1.6.7 since if R is Noetherian and dimension 0, then it is a semilocal ring.

For (3), let M be an R-oriented module, that is $\wedge^n M = R$ for some $n \geq 1$. Then by Corollary 1.6.10 M is projective and so by Bass cancellation theorem [Wei13, Theorem I.2.3], $M \cong P \oplus R^{n-1}$ for some projective module P of rank 1. Now

$$R = \wedge^n M = \wedge^n \left(P \oplus R^{n-1}\right) = \bigoplus_{k=0}^{n} \wedge^k P \otimes \wedge^{n-k} R^{n-1} = P \otimes R = P,$$

so M is free. Hence every finitely generated R-oriented module is free, so R is an OP-ring by Theorem 1.6.8.

□

Example 1.6.16. Let A be a PID with quotient field F and K/F be a finite field extension. An A-order R in K is an A-subalgebra of K which is finitely generated as an A-module and such that $F \otimes_A R = K$. In [Cla18, Theorem 3.4], Clark showed that if $N := [K : F]$, then there exists an A-order R in K such that R admits a maximal ideal $\mathfrak{m} \subset R$ with N as the minimal cardinality of a set of generators. If $N \geq 3$, then by Theorem 1.6.14 (6), R is not an OP ring. In particular if $K/\mathbb{Q}$ is a number field of degree at least 3, then K admits a $\mathbb{Z}$-order which is not an OP ring.

Note that if R is an A-order in a quadratic extension K/F, then every ideal of R is a free A-module of rank 2, so every maximal ideal of R is generated by at most 2 elements. Hence for any maximal ideal $\mathfrak{m} \subset R$, $\mathfrak{m}R_{\mathfrak{m}}$ is generated by at most 2 elements, so by Theorem 1.6.5, R is locally OP. Moreover, R is also a dimension 1 domain, so by Corollary 1.6.15 (3)(a), R is an OP ring.

From here on, we will work with the case where the ring R is a k-algebra for some field k. As we will see later, this will allow us to utilise the geometry of $\mathrm{Spec}(R)$ as a k-variety. The next theorem gives examples of k-algebras R where every stably-free projective module is free.

Theorem 1.6.17. *Let k be a ring, and R be a finitely generated 2 dimensional k-algebra. Then every finitely generated stably-free projective R-module is free if any of the following is satisfied:*

1. *k is an algebraically closed field [MS76, Theorem 1].*
2. *k is an infinite perfect field with $\mathrm{k} \neq 2$ and the cohomological dimension of k is at most 1 [Bha03, Remark 4.2].*
3. *k is a real closed field and all k-points on $\mathrm{Spec}(R)$ lie on a closed subscheme of dimension ≤ 1 [MS76, Theorem 3.1].*
4. *$k = \mathbb{Z}$ or $k = \mathbb{F}_q$ for any prime power q [MMR88, Corollary 2.5].*

Corollary 1.6.18. *Let k be a ring and R be a Noetherian reduced finitely generated 2 dimensional k-algebra satisfying one of the conditions (1)-(4) in Theorem 1.6.17. Then every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator if and only if every maximal ideal of R can be generated by two elements.*

Proof. Follows from applying Theorem 1.6.17 to the equivalence of (1) and (6) in Theorem 1.6.8. □

If R is a regular 2-dimensional finitely generated k-algebra with k algebraically closed, then R is locally OP-ring byCorollary 1.6.6, and every finitely generated stably-free projective module is free by Theorem 1.6.17 (1). Hence to apply (5) in Theorem 1.6.14 we only need to know whether $SK_0(R) = 0$. This can be rephrased into a question about zero cycles of a projective closure of $\mathrm{Spec}(R)$ by Theorem 1.6.19.

Recall that for a variety X/k, the Chow group $A_0(X)$ is the group of zero cycles of degree 0 modulo rational equivalence. For a projective variety X/k, we have the *Albanese map*

$$AJ_X : A_0(X) \to \mathrm{Alb}_{X/k}(k),$$

where $\mathrm{Alb}_{X/k}$ is the Albanese variety of X/k (see [SS03, Section 3] for more details about the Albanese map). We denote the kernel as $SA_0(X) := \ker AJ_X$, which is also denoted as $T(X)$ or $F^2CH_0(X)$ in some literature.

Theorem 1.6.19 (Theorem 3 [MS76]). *Let $V = \mathrm{Spec}(R)$ be a regular irreducible affine surface over an algebraically closed field k, and let X/k be a regular projective surface birationally equivalent to V. If $SA_0(X)$ is finite, then $SK_0(R) = 0$.*

Putting the above theorems together, we have the following corollary.

Corollary 1.6.20. *Let k be an algebraically closed field. Suppose R is a 2-dimensional regular domain that is a k-algebra. If $\mathrm{Spec}(R)$ is an open affine subvariety of a regular projective surface X/k with finite $SA_0(X)$, then R is an OP-ring, and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.*

Proof. This follows from combining the above theorems. Firstly, R is a locally OP-ring by Corollary 1.6.6, and by Theorem 1.6.19, $SK_0(R) = 0$. Finally, by Theorem 1.6.17 (1), every stably-free projective R-module is free, so R satisfies Theorem 1.6.14 (5). Hence R is an OP-ring and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator. □

When $k = \overline{\mathbb{F}}_p$, we have the following theorem describing the projective modules over k-algebras, which we use to give examples of OP-rings in Theorem 1.6.23.

Theorem 1.6.21 (Theorem 6.4.1 [KS07]). *Let R be a finitely generated algebra of dimension $d > 1$ over the algebraic closure of a finite field. Then any projective R-module of rank d has a non-zero free direct summand.*

Corollary 1.6.22. *Let R be a locally OP dimension 2 finitely generated $\overline{\mathbb{F}}_p$-algebra that satisfies one of the following:*

1. *R is reduced,*
2. *every minimal ideal of R is principal, or*
3. *R has only finitely many maximal ideals with non-regular localisation.*

Then R is an OP-ring and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.

Proof. By Theorem 1.6.8, we only need to show that every finitely generated oriented R-module is free. Let P be an oriented module of rank n. If $n > 2$ then by Bass cancellation theorem [Wei13, Theorem I.2.3], $P \cong Q \oplus R^{n-2}$ where Q is a projective module of rank 2. By Theorem 1.6.21, Q has a non-zero free direct summand, so $Q \cong Q' \oplus R$ for some finitely generated R-module Q'. Now

$$R = \wedge^n P = \wedge^n \left(Q' \oplus R^{n-1}\right) = \bigoplus_{k=0}^{n} \wedge^k Q' \otimes \wedge^{n-k} R^{n-1} = Q' \otimes R = Q'.$$

Hence P is free. □

Theorem 1.6.23. *Let R be a regular finitely generated $\overline{\mathbb{F}}_p$-algebra of dimension 2. Then R is an OP-ring and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.*

Proof. R is locally OP by Corollary 1.6.6, and R is regular so it is reduced. Hence R is an OP ring by Corollary 1.6.22, and so every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator. □

For an algebra over a characteristic 0 field, we have the following result for a graded $\overline{\mathbb{Q}}$-algebra.

Theorem 1.6.24 (Theorem 1.2 [KS02])**.** *Let $R = \oplus_{n\geq 0} R_n$ be a 2-dimensional graded normal Noetherian domain that is an associative algebra over $R_0 = \overline{\mathbb{Q}}$. Then every finitely generated projective module over R is free.*

Corollary 1.6.25. *Let $R = \oplus_{n\geq 0} R_n$ be a 2-dimensional regular graded domain that is an associative algebra over $R_0 = \overline{\mathbb{Q}}$. Then R is an OP ring, and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.*

Proof. Since R is a regular 2-dimensional ring, R is locally OP by Corollary 1.6.6. By Theorem 1.6.24, every finitely generated projective R-module is free, so every R-oriented module is free. Hence R is an OP ring by Theorem 1.6.8, and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator. □

Recall the following conjecture (see [KS07, Page 267 and Theorem 6.2.1] for a discussion about the conjecture).

Conjecture 1.6.26 (Bloch–Beilinson Conjecture). If $X/\overline{\mathbb{Q}}$ is an irreducible regular projective surface, then $SA_0(X) = 0$.

Theorem 1.6.27. *Assume the Bloch–Beilinson conjecture. Then every finitely generated dimension 2 regular $\overline{\mathbb{Q}}$-algebra R is an OP-ring. In particular, every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.*

Proof. For any R as in the theorem, there exists an irreducible regular projective surface $X/\overline{\mathbb{Q}}$ birational to $\mathrm{Spec}(R)$. By Conjecture 1.6.26, $SA_0(X) = 0$, so $SK_0(R) = 0$ by Theorem 1.6.19. By Theorem 1.6.17 (1), every stably-free projective module is free. Finally, R is locally OP since R is regular and dimension 2. Hence R satisfies Theorem 1.6.14 (5) so R is an OP-ring, and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator. □

In contrast to the case of $\overline{\mathbb{Q}}$-algebras, Corollary 1.6.29 gives examples of dimension 2 regular $\mathbb{C}$-algebras which are not OP-rings.

Theorem 1.6.28 (Mumford, Roitman, Corollary 1 [KS10])**.** *Let $X/\mathbb{C}$ be an irreducible regular proper variety of dimension d, with $H^0(X, \Omega^d_{X/\mathbb{C}}) \neq 0$. Let $\mathrm{Spec}(R)$ be a non-empty open affine subvariety of X. Then $A_0(\mathrm{Spec}\ R)$ has uncountable rank.*

Corollary 1.6.29. *Let $X/\mathbb{C}$ be an irreducible regular proper surface, with $H^0(X, \Omega^2_{X/\mathbb{C}}) \neq 0$, and let $\mathrm{Spec}(R)$ be a non-empty open affine subvariety of X. Then R is not an OP ring and there is a trace 0 non-commutator in $\mathrm{M}_2(R)$.*

Proof. By Theorem 1.6.28, $A_0(\mathrm{Spec}\ R) \neq 0$. Since $\mathrm{Spec}(R)$ is a regular affine surface, $A_0(\mathrm{Spec}\ R) = SK_0(R)$ (see Theorem 4.2 (d) [MS76]) and so it does not satisfy Theorem 1.6.14 (5). Hence R is not an OP ring and there exists a trace 0 non-commutator in $\mathrm{M}_2(R)$. □

Example 1.6.30. For any $d \geq 1$, let $R_d := \mathbb{C}[x, y, z]/(x^d + y^d + z^d - 1)$. Then $\mathrm{Spec}(R_d)$ is an open subvariety of $X_d := \mathrm{Proj}(\mathbb{C}[x_0, x_1, x_2, x_3]/(x_0^d + x_1^d + x_2^d + x_3^d))$. If $d = 1, 2, 3$, X_d is rational [Har77, Example II.8.20.3], and so $A_0(X_d) = 0$ [Blo10, Prop. 7.1]. Hence $SA_0(X_d) = 0$ and by Corollary 1.6.20, R_d is an OP-ring and every trace 0 matrix in $\mathrm{M}_2(R_d)$ is a commutator.

If $d \geq 4$, then we have $\Omega^2_{X_d/\mathbb{C}} = \mathcal{O}_{X_d}(d-4)$ (see [Har77, Example II.8.20.3]), so $H^0(X_d, \Omega^2_{X_d/\mathbb{C}}) = H^0(X_d, \mathcal{O}_{X_d}(d-4)) \neq 0$. Hence by Corollary 1.6.29, there is a trace 0 non-commutator in $\mathrm{M}_2(R_d)$. Note that if the Bloch-Beilinson conjecture is true, then $\overline{\mathbb{Q}}[x,y,z]/(x^d+y^d+z^d-1)$ is an OP-ring by Theorem 1.6.27 even if $d \geq 4$.

Recall the following conjecture of Bloch (see Conjecture 1.8 and Proposition 1.11 in [Blo10] for details about the conjecture).

Conjecture 1.6.31 (Bloch Conjecture). Let $X/\mathbb{C}$ be a regular projective surface. If $H^0(X, \Omega^2_{X/\mathbb{C}}) = 0$ then $SA_0(X) = 0$.

Bloch's conjecture has been verified in many cases, including for any surfaces that are not of general type [BKL76, Proposition 4] and for some surfaces of general type, see e.g. [Bau+12; IM79; Bar85; Voi14; Bau14; BF15; PW16]. Thus in these cases, we can apply Corollary 1.6.20 to obtain examples of OP-rings. For example, the following is an OP-ring coming from a surface of general type called a Godeaux surface.

Example 1.6.32. Let Y be the quintic complex surface in $\mathbb{P}^3_{\mathbb{C}}$ defined by the equation $x_0^5+x_1^5+x_2^5+x_3^5 = 0$. Let

$$\sigma(x_0 : x_1 : x_2 : x_3) = (x_0 : \zeta_5 x_1 : \zeta_5^2 x_2 : \zeta_5^3 x_3)$$

be an automorphism of Y where $\zeta_5 = e^{2\pi i/5}$. The quotient surface $X := Y/\langle\sigma\rangle$ is called a Godeaux surface, with $A_0(X) = 0$ (see [IM79, Theorem 1]).

So for an open affine subvariety $\mathrm{Spec}(R)$ of X, we have that R is an OP-ring by Corollary 1.6.20. For example consider

$$S := \mathbb{C}[x,y,z]/(x^5+y^5+z^5+1),$$

where $x := x_1/x_0$, $y := x_2/x_0$ and $z := x_3/x_0$, so that $\mathrm{Spec}(S)$ is an open subscheme of Y. Then σ acts on $\mathrm{Spec}(S)$ as well by $\sigma(f(x,y,z)) = f(\zeta_5 x, \zeta_5^2 y, \zeta_5^3 z)$, so $\mathrm{Spec}(S^{\langle\sigma\rangle}) \cong \mathrm{Spec}(S)/\langle\sigma\rangle$ is an open affine subvariety of X. Hence for

$$R := \left(\mathbb{C}[x,y,z]/(x^5+y^5+z^5+1)\right)^{\langle\sigma\rangle},$$

every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator.

We conclude this section with the case when $\mathrm{Spec}(R)$ is an affine quadric hypersurface in $\mathbb{A}^3_k$. We do not assume that k is algebraically closed, and use the theory of quadratics forms to determine whether R is an OP ring.

Given k a field with $\mathrm{char}\, k \neq 2$ and a homogeneous degree 2 polynomial $q(x, y, z) \in k[x, y, z]$, define

$$R(k, q) := k[x, y, z]/(q - 1).$$

Recall that q can be written as $q = (x \;\; y \;\; z)Q(x \;\; y \;\; z)^t$ where $Q \in \mathrm{M}_3(k)$ is a symmetric matrix. The *discriminant* of q is $\Delta(q) := \det(Q)$ and q is called *non-degenerate* if $\Delta(q) \neq 0$. If q is non-degenerate, then $R(k, q)$ is a regular 2-dimensional algebra. Finally, recall that q is *isotropic over* k if there exist $x, y, z \in k$ not all 0 such that $q(x, y, z) = 0$.

Theorem 1.6.33 (Theorem 16.1 [Swa87])**.** *Let $q \in k[x, y, z]$ be a non-degenerate quadratic form over a field k with $\mathrm{char}\, k \neq 2$. If q is isotropic or $\sqrt{-\Delta(q)} \in k$, then every projective $R(k, q)$-module with rank at least 1 has the form $F \oplus Q$ with F free and Q of rank 1.*

Corollary 1.6.34. *If q is isotropic or $\sqrt{-\Delta(q)} \in k$, then $R(k, q)$ is an OP-ring. Hence every trace 0 matrix in $\mathrm{M}_2(R(k, q))$ is a commutator.*

Proof. Let $R := R(k, q)$. Since R is a regular dimension 2 ring, it is a locally OP ring by Corollary 1.6.6. Now suppose P is an R-oriented projective module with $\wedge^n P = R$. Then by Theorem 1.6.33, $P = R^{n-1} \oplus Q$ with $\mathrm{rk}\, Q = 1$. So

$$R = \wedge^n P = \wedge^n (R^{n-1} \oplus Q) = R \otimes Q = Q.$$

Hence P is a free module, and by Theorem 1.6.14, R is an OP ring and every trace 0 matrix in $\mathrm{M}_2(R)$ is a commutator. □

We also have a partial converse of Theorem 1.6.33.

Theorem 1.6.35 (Theorem 9.2 (b) and Lemma 11.5 in [Swa87]). *If q is anisotropic, $\sqrt{-\Delta(q)} \notin k$ and q represents 1, then $\mathrm{Pic}(R(k,q)) = 0$ and $\tilde{K}_0(R(k,q)) = \mathbb{Z}/2\mathbb{Z}$.*

Corollary 1.6.36. *If q is anisotropic, $\sqrt{-\Delta(q)} \notin k$ and q represents 1, then $R(k,q)$ is not an OP-ring and there is a trace 0 matrix in $\mathrm{M}_2(R(k,q))$ that is not a commutator.*

Proof. Let $R := R(k,q)$. Since

$$SK_0(R) = \ker(\tilde{K}_0(R) \to \mathrm{Pic}(R)),$$

$SK_0(R) = \mathbb{Z}/2\mathbb{Z}$ by Theorem 1.6.35. Hence by Theorem 1.6.14, R is not an OP ring and there is a trace 0 matrix in $\mathrm{M}_2(R)$ that is not a commutator. □

Remark 1.6.37. Over $R := \mathbb{R}[x,y,z]/(x^2+y^2+z^2-1)$, there is a well-known example of a 2×2 non-commutator $A := \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \in \mathrm{M}_2(R)$ (see [RR00, Section 3] for the proof). By taking $q := x^2 + y^2 + z^2$ as the quadratic form, we see that $R = R(\mathbb{R}, q)$. Since $\sqrt{-\Delta(q)} = \sqrt{-1} \notin \mathbb{R}$, Corollary 1.6.36 implies that there is a non-commutator in $\mathrm{M}_2(R)$. However we cannot conclude from Corollary 1.6.36 that this particular matrix A is a non-commutator.

Note that for $R \otimes_{\mathbb{R}} \mathbb{C} = R(\mathbb{C}, q) = \mathbb{C}[x,y,z]/(x^2+y^2+z^2-1)$, Corollary 1.6.34 applies since $\sqrt{-\Delta(q)} = \sqrt{-1} \in \mathbb{C}$, so A is a commutator in $\mathrm{M}_2(R(\mathbb{C}, q))$. For example, we can write A as

$$A = \left[\begin{pmatrix} 1 + ix(ix-y) & -xz \\ x(ix-y) & 0 \end{pmatrix}, \begin{pmatrix} -iz & ix+y \\ -z & 0 \end{pmatrix} \right].$$

Remark 1.6.38. There are cases that are not covered by Corollary 1.6.34 and Corollary 1.6.36. Namely the case where q is anisotropic, $\sqrt{-\Delta(q)} \notin k$ and q does not represent 1. We now provide an explicit example of such form q. Take $k := \mathbb{Q}(a,b,c)$, a function field in 3 variables over $\mathbb{Q}$. Take $q := ax^2 + by^2 + cz^2 \in k[x,y,z]$. Then we claim that q is anisotropic, $\sqrt{\Delta(q)} \notin k$ and q does not represent 1. So suppose there

exist $x, y, z \in k$ such that

$$ax^2 + by^2 + cz^2 = 0. \tag{1.3}$$

Then by clearing the denominators, we may assume $x, y, z \in \mathbb{Q}[a, b, c]$. Now if we evaluate a, b, c in Equation (1.3) at any positive $a_0, b_0, c_0 \in \mathbb{Q}$, then we have $x(a_0, b_0, c_0) = 0$, $y(a_0, b_0, c_0) = 0$ and $z(a_0, b_0, c_0) = 0$. Hence x, y and z must all be 0 in $\mathbb{Q}[a, b, c]$ and so q is anisotropic. We can also see that $\sqrt{-\Delta(q)} = \sqrt{-abc} \notin k = \mathbb{Q}(a, b, c)$. Now we will show that q does not represent 1. So suppose by contradiction that it does represent 1. Then after clearing the denominators, we have

$$af_1^2 + bf_2^2 + cf_3^2 = f_4^2 \tag{1.4}$$

for some $f_1, f_2, f_3, f_4 \in \mathbb{Q}[a, b, c]$. We may also assume that Equation (1.4) is reduced in the sense that at least one of the f_i is not divisible by a, and similarly for b and c. Now suppose f_2, f_3, f_4 are all divisible by a. Then f_1 is not divisible by a, and after dividing Equation (1.4) by a and then taking modulo a, we will have

$$f_1^2 \equiv 0 \pmod{a}.$$

This is a contradiction since we assumed a does not divide f_1, so at least one of f_2, f_3, f_4 is not divisible by a. Suppose $f \in \{f_2, f_3, f_4\}$ is the only polynomial not divisible by a. Then taking Equation (1.4) modulo a, we will have

$$f^2 \equiv 0 \pmod{a},$$

which is a contradiction since we assumed a does not divide f. Hence there are at least two polynomials in f_2, f_3, f_4 that are not divisible by a. Similarly, there are 2 polynomials in f_1, f_3, f_4 that are not divisible by b and two polynomials in f_1, f_2, f_4 that are not divisible by c. So there is at least one polynomial in f_1, f_2, f_3, f_4 that is not divisible by a and b, a and c, or b and c. Without loss of generality, assume that at least one of f_3 or f_4 is not divisible by a and b. Then taking Equation (1.4) modulo (a, b), we have

$$cf_3^2 \equiv f_4^2 \mod (a, b).$$

This is an equation in $\mathbb{Q}[a,b,c]/(a,b) = \mathbb{Q}[c]$, and the only solution is $f_3 = 0 = f_4$ in $\mathbb{Q}[c]$. But this is a contradiction since we assumed at least one of f_3 or f_4 is not 0 modulo (a,b). Hence there is no f_1, f_2, f_3, f_4 satisfying Equation (1.4) and $q = ax^2 + by^2 + cz^2$ does not represent 1 in $k = \mathbb{Q}(a,b,c)$.

Chapter 2

Integer Dynamics

2.1 Introduction

In this chapter, we include [Lor+20], a joint work with D. Lorenzini, M. Melistas, A. Suresh, and H. Wang. Fix an integer $b \geq 2$. Any non-negative integer n can be written uniquely in base b as $n = x_0 + x_1 b + \cdots + x_d b^d$ with $x_d > 0$ and $0 \leq x_i < b$ for $i = 0, \ldots, d$. We let $n = [x_0, \ldots, x_d]_b$ denote the base b expansion of n. Fix now a function $\phi : \{0, 1, \ldots, b-1\} \to \mathbb{Z}_{\geq 0}$, and consider the map $S_{\phi,b} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$, with

$$S_{\phi,b}(n) := \phi(x_0) + \cdots + \phi(x_d).$$

For instance, when $b = 10$ and $\phi(x) = x^2$, then $S_{\phi,b}(345) = 3^2 + 4^2 + 5^2$.

The ordered sequence $[n, S_{\phi,b}(n), S_{\phi,b}(S_{\phi,b}(n)), \ldots]$ is called the *orbit* of n under $S_{\phi,b}$. We say that n has *finite orbit* under $S_{\phi,b}$ if the set $\{n, S_{\phi,b}(n), S_{\phi,b}(S_{\phi,b}(n)), \ldots\}$ is finite. Any finite orbit contains a finite *cycle*, a non-empty sequence of integers $\mathrm{cyc}(n_1, \ldots, n_\ell)$ such that $S_{\phi,b}(n_\ell) = n_1$ and when $\ell > 1$, $S_{\phi,b}(n_i) = n_{i+1}$ for $i = 1, \ldots, \ell - 1$. This cycle of *length* ℓ is unique up to cyclic permutation of its terms.

Example 2.1.1. Let $\phi(x) = x^2$ and $b = 10$. Take the integer $c := 142113251819$, which is obtained from *numbers* by substituting each letter with its position in the alphabet. The repeated use of the function

$S_{\phi,b}$ quickly brings c to a standstill: the orbit of c is $[c, 208, 68, 100, 1, 1, \dots]$, and the cycle associated to this orbit is $[1]$.

B. M. Stewart [Ste60, Theorem 1] proved that *there exists a constant γ, depending on ϕ, such that if $n > \gamma$, then $n > S_{\phi,b}(n)$. In particular every positive integer n has finite orbit under $S_{\phi,b}$.* It follows from Stewart's Theorem that the orbits of $S_{\phi,b}$ produce only finitely many distinct cycles. We will call the set of distinct cycles associated with the orbits of $S_{\phi,b}$ *the cycles associated with $S_{\phi,b}$*. The complete determination of the cycles of a given $S_{\phi,b}$ is computationally quite expensive for large b's. When $\phi(x) = x^m$, one can proceed as follows.

Theorem 2.1.2. *Let $\phi(x) = x^m$. For each integer $n \leq (m-1)b^m - 1$, compute the cycle of $S_{\phi,b}(n)$. Then the union of all these cycles is the complete set of cycles associated with $S_{\phi,b}$.*

This statement follows from [Ste60, Theorem 7], and the key to Stewart's proof is that if $n > (m-1)b^m - 1$, then $n > S_{\phi,b}(n)$. Hence, *every cycle for $S_{\phi,b}$ contains a positive integer at most equal to $(m-1)b^m - 1$. In particular, every cycle for $S_{\phi,b}$ contains a positive integer whose base b expansion has at most $m+1$ digits.*

When $\phi(x) = x^2$, the number of 1-cycles of a given $S_{x^2,b}$ is explicitly determined by the following theorem of P. Subramanian [Sub68, Theorem 1.2] (see also [HP78, Section 3], and Proposition 2.4.1). Recall that a divisor d of a positive integer n is called *proper* if $1 \leq d < n$.

Theorem 2.1.3. *The number of 1-cycles of $S_{x^2,b}$ is equal to the number of proper divisors of $b^2 + 1$.*

For convenience, let us call $[1]$ the *trivial* cycle of $S_{x^m,b}$. Let $\ell \geq 1$ be any integer. Let $B(\ell)$ denote the set of bases b such that $S_{x^2,b}$ has at least one non-trivial cycle of length ℓ. Theorem 2.1.3 implies that the natural density of $B(1)$ is 1 (see Remark 2.2.11). It is not hard to show that $B(\ell)$ is infinite for all ℓ (see Example 2.2.1), and it is natural to wonder whether $B(\ell)$ has a positive natural density. Let $S \subset \mathbb{N}$ is any subset. Let $S(n) := \{1, 2, \dots, n\} \cap S$ and $s(n) := |S(n)|$. Recall that the *lower density* $\underline{d}(S)$ of S is defined as $\underline{d}(S) := \liminf_{n\to\infty} \frac{s(n)}{n}$. In this chapter, we show:

Theorem (see Corollary 2.2.8 and Proposition 2.2.12). *Let $\ell \geq 1$. Then $B(\ell)$ has a positive lower density. More precisely, $B(\ell)$ always contains an explicit arithmetic progression. The sets $B(2)$, $B(3)$, and $B(4)$ have lower density bounded below by 0.57, 0.21, and 0.11, respectively.*

The key ingredient in the proof of Corollary 2.2.8 is the existence of special ℓ-cycles that we now define. Let $c = \mathrm{cyc}(n_1, \ldots, n_\ell)$ denote a cycle of length ℓ for $S_{x^2,b}$. We say that c is a *propagating cycle* if (i) every integer n_i, $i = 1, \ldots, \ell$, has at most two digits when written in base b and (ii) b does not divide n_i, for all $i = 1 \ldots, \ell$. The name 'propagating' is justified by our next theorem. It is easy to check with Theorem 2.1.2 that all 1-cycles of $S_{x^2,b}$ are propagating.

Theorem (see Theorem 2.2.7). *Let $b_0 \geq 2$. Assume that S_{x^2,b_0} has s distinct propagating cycles, of lengths $\ell_1, \ldots, \ell_s$, respectively (repetitions are allowed). Let $t \geq 0$ be any integer, and let $b := b_0 + t(b_0^2 + 1)$. Then $S_{x^2,b}$ has (at least) s distinct propagating cycles, of lengths $\ell_1, \ldots, \ell_s$ respectively.*

Propagating ℓ-cycles can naturally be seen as corresponding to integer points on an algebraic variety $V_\ell/\mathbb{Q}$. It turns out that V_ℓ has the property that, through every integer point on it corresponding to an ℓ-cycle, there passes at least one integer line given by explicit equations. This arithmetico-geometrical fact underlies the proof of Theorem 2.2.7. When $\ell = 1$ or 2, there is in addition a second integer line passing through each point which also propagates cycles. We exploit the existence of this second line when $\ell = 2$ in Proposition 2.3.4 and Remark 2.3.6.

Some of Stewart's 1960 results [Ste60] have been independently rediscovered by H. Hasse and G. Prichett in 1978 ([HP78, Theorem 4.1]). At the end of [HP78], Hasse and Prichett propose the following conjecture:

Let $\phi(x) = x^2$ and consider the set $L(x^2, 2)$ of all integers $b \geq 2$ such that the list of cycles associated with $S_{\phi,b}$ consists of the trivial cycle $[1]$ and exactly one additional cycle. Then $L(x^2, 2) = \{6, 10, 16, 20, 26, 40\}$.

Hasse and Prichett made this conjecture after having numerically verified it for $b \leq 500$.

Let $\phi(x)$ be any polynomial taking positive values on $\mathbb{Z}_{>0}$. Let $L(\phi, i)$ denote the set of integers $b \geq 2$ such that the list of cycles associated with $S_{\phi,b}$ consists of exactly i distinct cycles. It is natural to wonder

whether the Hasse–Prichett conjecture for $\phi(x) = x^2$ and $i = 2$ is in fact only a specific instance of a much more general phenomenon, namely that all the sets $L(\phi, i)$ are finite, for all $i \geq 1$.

Curiously, Hasse and Prichett do not mention in [HP78] a similar conjecture for the set $L(x^2, 1)$. In this case, that $L(x^2, 1) = \{2, 4\}$ seems to be by now a folklore conjecture. It is stated in [OEIS], A161872, that the conjecture has been verified for all $b < 500,000,000$.

Subramanian's Theorem 2.1.3 shows that if the set $L(x^2, 2)$ is infinite, it will indeed be very sparse, since if $b \in L(x^2, 1)$ or $L(x^2, 2)$, then $b^2 + 1$ is prime. To justify this claim, note that Theorem 2.1.3 implies that $b^2 + 1$ can only have at most one proper divisor bigger than 1. This can happen only when $b^2 + 1 = p^2$ for some prime p. But the factorisation $1 = (p - b)(p + b)$ has no integer solutions when $b \geq 2$.

The unboundedness of the set of integers b such that $b^2 + 1$ is prime is implied by a general 1857 conjecture of Victor Bouniakowsky [Bou57, page 328], that any irreducible polynomial $f(x) \in \mathbb{Z}[x]$ with positive leading coefficient takes infinitely many prime values if the values $f(1)$, $f(2)$, $f(3)$, ... have no common factor. This conjecture in the case of $f(x) = x^2 + 1$ was one of E. Landau's four problems presented at the 1912 International Congress of Mathematicians (see [HL23], pp 46-48). Note that a *negative* answer to the Hasse–Prichett Conjecture (in the strong sense where $L(x^2, 2)$ would be proved to be infinite) would provide a positive answer to Landau's problem.

The computations below were done using the cluster Sapelo2 at the Georgia Advanced Computing Resource Center. We have included the code used in Appendix A.

Theorem 2.1.4. *Let $b \leq 1000000$. If $b \in L(x^2, 2)$, then*

$$b \in \{6, 10, 16, 20, 26, 40, 8626, 481360\}.$$

Thus the Hasse–Prichett Conjecture at the very least needs to be modified to include the bases $b = 8626$ and $b = 481360$. The existence of the large gap between these two bases might be seen as evidence against the validity of the modified conjecture.

Searching for other types of finiteness, one may wonder for instance whether, for a given integer d, the set $M(x^2, d)$ of all bases b such that $S_{x^2,b}$ only has cycles of length at most d is finite. We have $\{2, 4\} \subseteq M(x^2, 1)$ and $\{2, 3, 4, 13, 18, 92\} \subseteq M(x^2, 2)$.

Theorem 2.1.5. *Let* $400 \leq b \leq 1100000$. *If* $b \in M(x^2, 10)$, *then*

$$b \in \{432, 596, 687, 1068, 1932, 3918, 288504\}.$$

Moreover, $452808 \in M(x^2, 12)$. The presence of the large gap in $M(x^2, 10)$ might be seen as evidence that $M(x^2, 10)$ might be infinite.

For comparison with the case $\phi(x) = x^2$, let us note the following results for $\phi(x) = x^3$.

Theorem (see Proposition 2.5.1 and Proposition 2.5.4). *Let* $b > 2$ *be a square, or an integer that is not divisible by* 9. *Then* $S_{x^3,b}$ *has at least one non-trivial* 1*-cycle. In particular, the set of bases* $b \geq 2$ *such that* $S_{x^3,b}$ *has a non-trivial* 1*-cycle has lower density bounded below by* $8/9$.

Theorem (see Proposition 2.5.7 and Corollary 2.6.3). Let $k \geq 1$ be any integer.

(a) *Let* $b = 3k + 1$. *Then* $S_{x^3,b}$ *has at least five distinct cycles.*

(b) *Let* $b = 9k^2 + 15k + 7$ *or* $9k^2 + 21k + 13$. *Then* $S_{x^3,b}$ *admits at least one* 2*-cycle.*

Part (a) of the above theorem can be interpreted as saying that at least $1/3$ of the integers do not belong to $L(x^3, i)$ with $i \leq 4$. In the spirit of the Hasse–Prichett conjecture, we offer the following questions in the case where $\phi(x) = x^3$: do the equalities $L(x^3, 1) = \{2\}$, $L(x^3, 2) = \varnothing$, $L(x^3, 3) = \{3, 26\}$, and $L(x^3, 4) = \{5, 90, 188\}$ hold?

2.2 Propagating ℓ-cycles

Let $\phi(x)$ be any polynomial taking positive values on $\mathbb{Z}_{>0}$, and let $\ell \geq 1$ be any integer. It is natural to wonder whether there exist bases $b \geq 2$ such that $S_{\phi,b}$ admits cycles of length ℓ. We consider this question in this section mainly when $\phi(x) = x^2$. We start with some general observations for $\phi(x) = x^m$, $m \geq 2$.

Example 2.2.1. Let $\ell > 1$ and $m \geq 2$ be any integers. Let $b := c^{m^\ell - 1}$. Then the orbit of c^m under $S_{x^m,b}$ is a cycle of length ℓ, namely the cycle $\mathrm{cyc}(c^m, c^{m^2}, \ldots, c^{m^\ell} = bc)$. Thus we can quantify the infinitude of the set of bases b such that $S_{x^m,b}$ contains a cycle of length ℓ by noting that this set contains all integer values of the polynomial $f(t) = t^{m^\ell - 1}$ when $t > 1$. We show in Corollary 2.2.8 that when $m = 2$, the same statement holds with a polynomial $f(t)$ of degree 1.

Example 2.2.2. Take a prime $p > m$, and let ℓ denote the order of m in $(\mathbb{Z}/p\mathbb{Z})^*$. We find that the base $b = c^p$ admits the orbit of c^m under $S_{x^m,b}$ as a cycle of length ℓ. Thus, when the order of m equals $\ell := p - 1$, we find that all integer values of the polynomial $f(t) = t^{\ell+1}$ when $t > 1$ are contained in the set of bases b such that $S_{x^m,b}$ contains a cycle of length ℓ.

For instance when $\ell = 4$ and $m = 2$, we have for all bases $b = c^5$ the 4-cycle $\mathrm{cyc}(c^2, c^4, c^8, c^6)$. When $\ell = 2$, we can consider the 2-cycle $\mathrm{cyc}(c^m, c^{m^2})$ in base $b = c^{m+1}$, since in base b, $c^{m^2} = c(c^{m+1})^{m-1}$.

Example 2.2.3. *Existence of propagating ℓ-cycles.* None of the examples of ℓ-cycles exhibited above when $\phi(x) = x^2$ are examples of propagating cycles as defined in the introduction, since although each integer in the cycle has at most two digits when written in base b, at least one integer in the cycle is divisible by b. Our next example is an example of a propagating cycle.

Fix $\ell \geq 2$. Choose coprime positive integers α and β such that β divides $\alpha^{2^\ell} - \alpha$, and set $\gamma := \alpha^2 + \beta^2$. For instance, one can choose $\alpha = \beta = 1$ and $\gamma = 2$. Set $b := (\gamma^{2^{\ell-1}} - \alpha)/\beta$. Since β divides $\alpha^{2^\ell} - \alpha$ and $\alpha^2 = \gamma - \beta^2$, we find that b is an integer. Then

$$\mathrm{cyc}(\gamma, \gamma^2, \gamma^4, ..., \gamma^{2^{\ell-1}} = \alpha + \beta b)$$

is an ℓ-cycle for $S_{x^2,b}$. Indeed, it is easy to verify that $\alpha, \beta < b$, so that $\gamma^{2^{\ell-1}} = [\alpha, \beta]_b$.

It is easy to check that b does not divide any of the integers γ^{2^k} for $k = 0, \ldots, \ell - 1$. Since $\gamma^{2^{\ell-1}}$ has only two digits in base b, the smaller integers γ^{2^k} have at most two digits. Hence, this cycle is a propagating cycle.

Let $\ell \geq 1$. Consider the affine space $\mathbb{A}^{2\ell+1}$ and label its coordinates by

$$b, \text{ and } x_i, y_i, \text{ for } i = 1, \ldots, \ell.$$

Let V_ℓ denote the algebraic subvariety of $\mathbb{A}^{2\ell+1}$ defined by $x_1^2 + y_1^2 = x_1 + by_1$ when $\ell = 1$, and in general by the ℓ equations

$$\begin{aligned} x_i^2 + y_i^2 &= x_{i+1} + by_{i+1} \quad \text{for } i = 1, \ldots, \ell - 1, \text{ and} \\ x_\ell^2 + y_\ell^2 &= x_1 + by_1. \end{aligned}$$

Let now $\mathrm{cyc}(n_1, \ldots, n_\ell)$ be a propagating ℓ-cycle for S_{x^2,b_0}. Write $n_i = [\mathbf{x}_i, \mathbf{y}_i]_{b_0}$ with $0 \leq \mathbf{x}_i, \mathbf{y}_i \leq b_0 - 1$ and $\mathbf{x}_i \neq 0$. Then the integer point $(b_0, \mathbf{x}_i, \mathbf{y}_i, i = 1, \ldots, \ell)$ satisfies the equations of the variety V_ℓ, and thus a propagating ℓ-cycle for S_{x^2,b_0} corresponds to an integer point on the variety V_ℓ which satisfies the added requirement that $0 \leq \mathbf{x}_i, \mathbf{y}_i \leq b_0 - 1$ and $\mathbf{x}_i \neq 0$.

Theorem 2.2.4. *Let $P := (b_0, \mathbf{x}_1, \mathbf{y}_1, \ldots, \mathbf{x}_\ell, \mathbf{y}_\ell)$ be any point on the variety V_ℓ. Then there exists a line in $\mathbb{A}^{2\ell+1}$ that passes through P and is fully contained in V_ℓ. This line can be given by the parametric equations*

$$\begin{aligned} b(t) &:= b_0 + (b_0^2 + 1)t, \\ x_i(t) &:= \mathbf{x}_i + (\mathbf{x}_i b_0 - \mathbf{y}_i)t, \\ y_i(t) &:= \mathbf{y}_i + (\mathbf{y}_i b_0 + \mathbf{x}_i)t, \textit{ for } i = 1, \ldots, \ell. \end{aligned} \tag{2.1}$$

If P is a point which corresponds to a propagating cycle of S_{x^2,b_0}, then for every non-negative integer $\mathbf{t}$, the point

$$P(\mathbf{t}) := (b(\mathbf{t}), x_1(\mathbf{t}), y_1(\mathbf{t}), \ldots, x_\ell(\mathbf{t}), y_\ell(\mathbf{t}))$$

corresponds to a propagating cycle for $S_{x^2,b(\mathbf{t})}$.

Proof. The proof of the theorem is not difficult, once the parametric equations (2.1) are available. Indeed, one finds that in $\mathbb{Q}[t]$,

$$\begin{aligned} x_i(t)^2 + y_i(t)^2 - x_{i+1}(t) - b(t)x_{i+1}(t) &= (\mathbf{x}_i^2 + \mathbf{y}_i^2 - \mathbf{x}_{i+1} - b_0\mathbf{y}_{i+1})((b_0t+1)^2 + t^2) \\ &= 0, \end{aligned}$$

for all $i = 1, \ldots, \ell$ (where the index $\ell + 1$ is set to mean index 1). We further need to show that for all $\mathbf{t} \geq 0, 0 \leq x_i(\mathbf{t}), y_i(\mathbf{t}) < b(\mathbf{t})$, and that $x_i(\mathbf{t}) \neq 0$. These inequalities follow from the the fact that since $\mathbf{x}_i \neq 0$ and $\mathbf{y}_i < b_0$, we have $\mathbf{x}_i b_0 - \mathbf{y}_i > 0$, $\mathbf{x}_i + b_0\mathbf{y}_i > 0$, and $(\mathbf{x}_i b_0 - \mathbf{y}_i), (\mathbf{x}_i + b_0\mathbf{y}_i) \leq b_0^2 - 1$. □

Remark 2.2.5. Consider an ℓ-cycle $\mathrm{cyc}(n_1, \ldots, n_\ell)$ as in Theorem 2.2.4, with $n_i := \mathbf{x}_i + \mathbf{y}_i b_0$. Let $g := \gcd(b_0^2 + 1, n_1, \ldots, n_\ell)$. Given the parametrisation (2.1), we will call the following parametrisation of the same line the *reduced integer parametrisation* of the line:

$$\begin{aligned} b(t) &:= b_0 + t(b_0^2 + 1)/g, \\ x_i(t) &:= \mathbf{x}_i + t(\mathbf{x}_i b_0 - \mathbf{y}_i)/g, \\ y_i(t) &:= \mathbf{y}_i + t(\mathbf{y}_i b_0 + \mathbf{x}_i)/g, \text{ for } i = 1, \ldots, \ell. \end{aligned}$$

Note that g divides $\mathbf{x}_i b_0 - \mathbf{y}_i$ since $\mathbf{x}_i b_0 - \mathbf{y}_i = b_0(\mathbf{y}_i b_0 + \mathbf{x}_i) - \mathbf{y}_i(b_0^2 + 1)$. Note also that $g < b_0^2 + 1$ since if $g = b_0^2 + 1$, then $b_0^2 + 1$ would divide $n_i := \mathbf{x}_i + \mathbf{y}_i b_0$, but this is not possible since $n_i \leq b_0^2 - 1$.

Remark 2.2.6. For each $\mathbf{t} \in \mathbb{C}$, we can define an endomorphism $\varphi_\mathbf{t} : V_\ell \to V_\ell$ on the affine variety V_ℓ using the ring homomorphism $\varphi_\mathbf{t}^*$ on functions on V_ℓ defined as:

$$\begin{aligned} \varphi_\mathbf{t}^*(b) &:= b + \mathbf{t}(b^2 + 1), \\ \varphi_\mathbf{t}^*(x_i) &:= x_i + \mathbf{t}(x_i b - y_i), \\ \varphi_\mathbf{t}^*(y_i) &:= y_i + \mathbf{t}(y_i b + x_i), \text{ for } i = 1, \ldots, \ell. \end{aligned}$$

Theorem 2.2.7. *Let $b_0 \geq 2$. Assume that S_{x^2,b_0} has s distinct propagating cycles, of lengths $\ell_1, \ldots, \ell_s$, respectively (repetitions are allowed). Let $\mathbf{t} \geq 0$ be any integer, and let $b := b_0 + \mathbf{t}(b_0^2+1)$. Then $S_{x^2,b}$ has (at least) s distinct propagating cycles, of lengths $\ell_1, \ldots, \ell_s$ respectively.*

Proof. When the integers $\ell_1, \ldots, \ell_s$ are distinct, the statement of the theorem follows immediately from the existence of the 'propagating' lines proved in Theorem 2.2.4. Suppose now that for some integer ℓ, there are exactly $j > 1$ indices i such that $\ell_i = \ell$. Since we start with j distinct propagating ℓ-cycles, we have j distinct points on V_ℓ, and Theorem 2.2.4 proved the existence of j distinct lines on V_ℓ. To conclude the proof of Theorem 2.2.7, it suffices to prove that these lines do not intersect in V_ℓ at a point where $\mathbf{t}$ is a positive integer. This can be checked directly. Assume that $\mathbf{t} \neq 0$, and that we have two ℓ-cycles $(b_0, \mathbf{x}_1, \mathbf{y}_1, \ldots)$ and $(b_0, \overline{\mathbf{x}_1}, \overline{\mathbf{y}_1}, \ldots)$ with

$$\begin{aligned} \mathbf{x}_i + (\mathbf{x}_i b_0 - \mathbf{y}_i)\mathbf{t} &= \overline{\mathbf{x}_i} + (\overline{\mathbf{x}_i} b_0 - \overline{\mathbf{y}_i})\mathbf{t}, \\ \mathbf{y}_i + (\mathbf{x}_i + \mathbf{y}_i b_0)\mathbf{t} &= \overline{\mathbf{y}_i} + (\overline{\mathbf{x}_i} + \overline{\mathbf{y}_i} b_0)\mathbf{t}, \end{aligned}$$

for $i = 1, \ldots, \ell$. Then

$$\begin{aligned} (\mathbf{x}_i - \overline{\mathbf{x}_i})(1 + b_0\mathbf{t}) &= (\mathbf{y}_i - \overline{\mathbf{y}_i})\mathbf{t}, \\ (\mathbf{y}_i - \overline{\mathbf{y}_i})(1 + b_0\mathbf{t}) &= -(\mathbf{x}_i - \overline{\mathbf{x}_i})\mathbf{t}. \end{aligned}$$

We must have $(\mathbf{x}_i - \overline{\mathbf{x}_i}) = 0$ and, hence, $(\mathbf{y}_i - \overline{\mathbf{y}_i}) = 0$, since otherwise, the above equations imply that $(b_0\mathbf{t} + 1)^2 + \mathbf{t}^2 = 0$. This latter equation is not possible when both $\mathbf{t}$ and b_0 are real, which we assume. □

Denote by $\mathrm{PB}(\ell)$ the set of bases $b \geq 2$ such that $S_{x^2,b}$ has a propagating ℓ-cycle.

Corollary 2.2.8. *Let $\ell \geq 2$. Let $b_0 := 2^{2^{\ell-1}} - 1$. Then the set $\mathrm{PB}(\ell)$ contains an arithmetic progression, and has lower density bounded below by $2/(b_0^2+1)$.*

Proof. The existence of a propagating ℓ-cycle $\mathrm{cyc}(\gamma, \gamma^2, \ldots)$ for the base $b_0 := 2^{2^{\ell-1}} - 1$ is established in Example 2.2.3. Since $\gamma = 2$, we find that the greatest common divisor of the elements in the cycle is 2. Theorem 2.2.4 and Remark 2.2.5 show the existence of an arithmetic progression $b(\mathbf{t}) = b_0 + \mathbf{t}(b_0^2+1)/2$

such that for every integer $\mathbf{t} \geq 1$, $S_{x^2,b(\mathbf{t})}$ has a propagating ℓ-cycle. The natural density of the set of positive integers in an arithmetic progression $\{a\mathbf{t} + b \mid \mathbf{t} \geq 0\}$ is $1/a$. □

Example 2.2.9. Every base b whose last digit in base 10 is 3 or 8 has a propagating 2-cycle. This follows from the fact that in base $b_0 = 3$, the 2-cycle $\mathrm{cyc}(2, 4)$ is propagating.

Remark 2.2.10. For later use, we note here the following facts. Consider a set S of positive integers which contains a union $U := \bigcup_{i=1}^{n} \left(\bigcup_{j=1}^{r_i} \{a_i t + b_{ij} \mid t \geq 0\} \right)$ of arithmetic progressions. Then the lower density $\underline{d}(S)$ of S satisfies $\underline{d}(S) \geq d(U)$. When the a_i are pairwise coprime, we find that

$$d(U) = 1 - \prod_{i=1}^{n} \left(1 - \frac{r_i}{a_i}\right).$$

Remark 2.2.11. Let us show now that $\mathrm{PB}(1)$ has natural density 1. More generally, let $f(x) \in \mathbb{Z}[x]$ be such that $f(\mathbb{Z}_{\geq 0}) \subseteq \mathbb{Z}_{\geq 0}$, and consider $B := \{b \in \mathbb{N} \mid f(b) \text{ is not prime}\}$. Subramanian's Theorem 2.1.3 shows that $\mathrm{PB}(1)$ has the same natural density as the set B when $f(x) = x^2 + 1$.

Let S denote the set of primes p such that there exists $b_p \in \mathbb{N}$ with $f(b_p)$ divisible by p. The set B then contains the arithmetic progression $b_p + pt$ for each $p \in S$. Thus the lower density of B is bounded below by the product $1 - \prod_{p \in S} \left(1 - \frac{1}{p}\right)$. The product $\prod_{p \in S} \left(1 - \frac{1}{p}\right)$ converges to 0 if and only if the sum $\sum_{p \in S} \frac{1}{p}$ diverges. When $f(x) = x^2 + 1$, the set S consists of 2 and all primes p congruent to 1 mod 4. It follows from Dirichlet's theorem on primes in arithmetic progression that $\sum_{p \in S} \frac{1}{p}$ diverges, so that the density of B is 1 in this case.

Proposition 2.2.12. *For $\ell = 2, 3, 4, 5$, the lower density $\underline{d}(\mathrm{PB}(\ell))$ is bounded below as follows:*

Table 2.1: Lower density of $\mathrm{PB}(\ell)$

ℓ	2	3	4	5
$\underline{d}(\mathrm{PB}(\ell)) \geq$	0.5763	0.2127	0.1144	0.0429

Proof. The steps in the computations of the four lower bounds given in the above table are the same for each ℓ. First compute a set P of propagating cycles. In our case, we used all propagating cycles with

$2 \leq b \leq 500$. For each propagating cycle $\mathrm{cyc}(n_1, n_2, \dots)$ in base b, Theorem 2.2.4 produces integer lines, which we parametrise using their reduced integer parametrisation (see Remark 2.2.5). The slope of each line is $\lambda := (b^2+1)/\gcd(b^2+1, n_1, n_2, \dots)$.

Thus we now have a set of explicit arithmetic progressions of the form $b + \lambda t$ which are contained in $\mathrm{PB}(\ell)$. To compute a lower bound for the lower density, we further prune the set of lines from all the lines which do not have prime power slope. The lower density of the set of arithmetic progressions with λ a prime power can be easily bounded below since the slopes are all pairwise coprime and we can use the formula in Remark 2.2.10 to obtain a lower bound for $\underline{d}(\mathrm{PB}(\ell))$. Our computations produce the following data:

Table 2.2: Number of propagating cycles and the lower density of $\mathrm{PB}(\ell)$

ℓ	1	2	3	4	5
$\lvert P\rvert$	2444	1163	391	190	77
$\underline{d}(\mathrm{PB}(\ell)) \geq$	0.8917	0.3507	0.2127	0.1144	0.0429

The data when $\ell = 1$ is only included for information, since we know already that $\underline{d}(\mathrm{PB}(1)) = 1$. The lower bound for $\underline{d}(\mathrm{PB}(2))$ is improved to $\underline{d}(\mathrm{PB}(2)) \geq 0.5763$ in Proposition 2.3.3. □

Remark 2.2.13. Computations indicate that the first integer b such that $S_{x^2,b}$ has a propagating ℓ-cycle might be much smaller than $2^{2^{\ell-1}} - 1$ when $\ell > 2$. One may wonder whether the first such b might even be bounded by a polynomial function in ℓ. Computations show that for each $\ell \leq 20$, there exists a basis $b \leq 1230$ with an ℓ-cycle.

Remark 2.2.14. Among the first 39000 bases b, only 1330, or about 3.41%, do not have a 2-cycle. The lower density of the set of bases b with a 2-cycle might thus be quite larger than 0.5763, and it would be interesting to determine if it is actually equal to 1. Among the first 25000 bases b, 17155, or about 68.62%, have a 3-cycle.

2.3 2-cycles for $S_{x^2,b}$

In addition to the line described in Theorem 2.2.4, both varieties V_1 and V_2 contain a second integer line through each integer point. We prove this fact in this section for the variety V_2 and exploit the existence of this second line to study the 2-cycles of $S_{x^2,b}$.

Proposition 2.3.1. *Let $P := (b_0, x_0, y_0, u_0, v_0)$ be any point with non-negative rational coefficients on the threefold V_2 (defined just before* Theorem 2.2.4*) outside of the lines $(t, 0, 0, 0, 0)$ and $(t, 1, 0, 1, 0)$. Then there exist two lines in $\mathbb{A}^5$, defined by equations with coefficients in $\mathbb{Q}$, which are entirely contained in V_2 and pass through P.*

Proof. Start with ten variables $x_0, x_1, y_0, y_1, u_0, u_1, v_0, v_1$, and b_0, b_1. Evaluate the two equations for V_2 at the linear polynomials $b(t) := b_0 + tx_1$, $x(t) := x_0 + tx_1$, $y(t) := y_0 + ty_1$, $u(t) := u_0 + tu_1$, and $v(t) := v_0 + tv_1$ to obtain two quadratic polynomials in t, say $f := f_2t^2 + f_1t + f_0$ and $g := g_2t^2 + g_1t + g_0$. Forcing these two polynomials to vanish identically produces six equations in the ten variables. The constant terms $f_0 = x_0^2 + y_0^2 - (u_0 + b_0v_0)$ and $g_0 = u_0^2 + v_0^2 - (x_0 + b_0y_0)$ are just the two equations of V_2 evaluated at the 0-variables.

Magma [BCP97] can verify that (f_0, g_0) is a prime ideal in $\mathbb{Q}[x_0, y_0, u_0, v_0, b_0]$. Let F denote the field of fractions of the ring $\mathbb{Q}[x_0, y_0, u_0, v_0, b_0]/(f_0, g_0)$. Consider the ideal $I := (f_1, f_2, g_1, g_2)$ in the polynomial ring $F[x_1, y_1, u_1, v_1, b_1]$. Use the Magma [BCP97] function `PrimaryDecomposition`(I) to produce the primary decomposition of this ideal. After about 34 hours of computing time, Magma will produce a decomposition which consists of three distinct ideals. Two of these ideals have generators that can be used to produce the parametric formulas for two different lines defined over $\mathbb{Q}$. Both lines at this point have parametric equations which are too long and complicated to be printed in this dissertation. We succeeded in simplifying the parametrisation of one of the lines, and checked that this line is the same line as the line exhibited in Theorem 2.2.4.

For the remainder of this section, let us call *the second line* through a point P on V_2 the line whose existence is established in the proposition and which is not equal to the line exhibited in Theorem 2.2.4.

The Magma computation allows us to give this line in parametric form

$$b(t) := b_0 + t \quad x(t) := x_0 + tX_1/D, \quad y(t) := y_0 + tY_1/D,$$
$$u(t) := u_0 + tU_1/D, \quad v(t) := v_0 + tV_1/D,$$

where the coefficients D, X_1, Y_1, U_1, V_1 are long formulas in the variables b_0, x_0, y_0, u_0, v_0. For instance,

$$\begin{aligned} D := u_0^2 + v_0^2 + 4y_0^2u_0^4 + 8y_0^2u_0^3 + 8y_0^2u_0^2v_0^2 + 4y_0^2u_0^2 + 8y_0^2u_0v_0^2 + 4y_0^2v_0^4 + 4y_0^2v_0^2 \\ +4y_0u_0^4v_0 + 8y_0u_0^2v_0^3 + 4y_0v_0^5 + u_0^6 + 2u_0^5 + 3u_0^4v_0^2 + 3u_0^4 + 4u_0^3v_0^2 + 2u_0^3 \\ +3u_0^2v_0^4 + 6u_0^2v_0^2 + 2u_0v_0^4 + 2u_0v_0^2 + v_0^6 + 3v_0^4, \end{aligned}$$

and we see that since D is a sum of monomials which includes $u_0^2 + v_0^2$, we must have $D > 0$ at P since the point P has non-negative coefficients and since u_0 and v_0 are not both zero by hypothesis. □

Remark 2.3.2. The line exhibited in Theorem 2.2.4 is remarkable since it allows us to 'propagate' any given propagating cycle. We believe that the second line on V_2 has the same property. In particular, starting with a propagating 2-cycle, we expect that the expressions X_1, Y_1, U_1, V_1 are all non-negative. This is immediately true for Y_1 since Magma produces a formula which is a sum of monomials, but for the other expressions, the formula involves some negative signs. The propagating property on the other hand can always be checked directly given an explicit propagating cycle, and this is what we do in order to establish our next proposition.

Assume that the point $P := (b_0, x_0, y_0, u_0, v_0)$ on V_2 has integer coefficients. Then the second lines can be parametrised using a change of variables of the form $t := \lambda s$ with $\lambda \in \mathbb{N}$ so that the new equations for the lines have only integer coefficients. In general there are very large cancellations in the fractions $X_1/D, Y_1/D, U_1/D$ and V_1/D and we set in this case λ to be the least common multiple of the denominators of $X_1/D, Y_1/D, U_1/D$ and V_1/D. We can use the second line through propagating 2-cycles to improve the lower bound given Proposition 2.2.12.

Proposition 2.3.3. *The set* $\mathrm{PB}(2)$ *of bases* $b \geq 2$ *such that* $S_{x^2,b}$ *has a propagating* 2*-cycle has lower density bounded below by* 0.5763*.*

Proof. Consider the set P_N of all propagating 2-cycles with $2 \leq b \leq N$. As in Proposition 2.2.12, for each propagating cycle $\mathrm{cyc}(n_1, n_2)$ in base b in P_N, Theorem 2.2.4 produces an integer line, which we parametrise using its reduced integer parametrisation (see Remark 2.2.5). The slope of the line is $\lambda_1 := (b^2+1)/\gcd(b^2+1, n_1, n_2)$. Consider the set S_1 of all the lines found this way.

Now for each propagating 2-cycle in base b in P_N, say $\mathrm{cyc}(x_0 + by_0, u_0 + bv_0)$, compute the reduced integer parametrisation of the second line, with $b(t) = b + \lambda_2 t$, $x(t) = x_0 + x_2 t$, $y(t) = x_0 + y_2 t$, $u(t) = u_0 + u_2 t$, and $v(t) = v_0 + v_2 t$, and check that this line allows us to propagate the 2-cycle. To check this, we verified that $0 \leq x_2, y_2, u_2, v_2 \leq \lambda_2$. Consider the set S_2 of all the second lines found this way. We now have a set of explicit arithmetic progressions of the form $b + \lambda_1 t$ or $b + \lambda_2 t$ which are contained in $\mathrm{PB}(2)$.

To compute a lower bound for the lower density, we further prune the set $S_1 \cup S_2$ from all the lines whose slope is not a power of a prime. The lower density of the set of arithmetic progressions associated with the remaining lines can be easily bounded below since the lines have slopes that are all pairwise coprime and we can use the formula in Remark 2.2.10 to obtain a lower bound of 0.5457 when $N = 1000$ and $|P_N| = 2885$. We can do slightly better by also considering some lines whose slope is not a power of a prime. For instance, when also considering the lines with slopes dividing $2 \cdot 17^3$, we obtain a lower bound of 0.5763 when $N = 1000$. □

Let $P = (b_0, x_0, y_0, u_0, v_0)$ be a propagating cycle on V_2, and consider the two lines passing through it and their reduced integer parametrisation with $b_1(t) = b_0 + \lambda_1 t$ and $b_2(t) = b_0 + \lambda_2 t$. We have noted already that $\lambda_1 = (b_0^2+1)/\gcd(b_0^2+1, n_1, n_2) > 1$, so that for any positive integer $\mathbf{t}$, $b_1^2(\mathbf{t}) + 1$ is never prime. Thus no propagated cycle on the first line can have a base b such that b^2+1 is prime. On the other hand, quite often, the second line can produce propagated cycles that have a base b such that b^2+1 is prime. Our next proposition exploits this property.

Proposition 2.3.4. (a) *There exist infinitely many integers $b \geq 2$ such that $S_{x^2,b}$ has exactly two non-trivial 1-cycles, but $b \notin L(x^2, 3)$ because $S_{x^2,b}$ also has a 2-cycle.*

(b) *The Bouniakowsky Conjecture implies that there exist infinitely many integers $b \geq 2$ such that $S_{x^2,b}$ has no non-trivial 1-cycles, but $b \notin L(x^2, 2)$ because $S_{x^2,b}$ also has two distinct 2-cycles.*

Proof. Part (a) follows from the existence of the second line on V_2 passing through the point $P := (8, 2, 3, 5, 1)$, and given by

$$b = 17t + 8, x = 3t + 2, y = 5t + 3, u = 9t + 5, v = 2t + 1.$$

Indeed, this line has $b(t) = 17t + 8$, with $\gcd(17, 65) = 1$. It follows from Lemma 2.3.5 that the integer values of $(17x + 8)^2 + 1$ are coprime and so we can use [Iwa78, Theorem, p. 172], fully proved in [Lem12, Theorem 1], applied to the polynomial $(17x + 8)^2 + 1$ to obtain that there are infinitely many values b in the arithmetic progression $b(t) = 17t + 8$ such that $b^2 + 1$ is the product of two primes. It is clear from the equation of the line that for every positive t, $S_{x^2,b(t)}$ has a propagating 2-cycle.

Part (b) follows from the existence of a second line with a similar property. Starting with the 2-cycle $(24, 16, 6, 4, 12)$, we find using the proof of Proposition 2.3.1 that the second line on V_2 through that point is given by

$$b = 53t + 24, x = 34t + 16, y = 13t + 6, u = 8t + 4, v = 25t + 12.$$

Again, all the coefficients of the line are positive, and it is easy to verify that for all $t > 0$, $x, y, u, v < b$. Thus for each t, the corresponding b is such that $S_{x^2,b}$ has a 2-cycle. It is easy to verify that $\gcd(53, 24^2 + 1) = 1$. Finally, we can find a point in the intersection of the arithmetic progressions $17t + 8$ and $53t + 24$; for instance when $x_0 = 400$ and $x_1 = 128$, we have $17x_0 + 8 = 53x_1 + 24 = 6808$. Thus we can consider the progression $17 \cdot 53t + 6808$, and Lemma 2.3.5 (b) shows that the integer values of $(17 \cdot 53x + 6808)^2 + 1$ are coprime. Hence, the Bouniakowsky Conjecture implies that there exist infinitely many integers t such that $(17 \cdot 53t + 6808)^2 + 1$ is prime and, therefore, there exist infinitely

many integers b of the form $b = 17 \cdot 53t + 6808$ such that $b^2 + 1$ is prime. For each such integer, we find that $S_{x^2,b}$ has two 2-cycles by construction. □

Lemma 2.3.5. (a) *Let $c, d \in \mathbb{Z}$. The integer values of the polynomial $(cx + d)^2 + 1$ are coprime if and only if $\gcd(c, d^2 + 1) = 1$.*

(b) *Let $c_0, d_0, c_1, d_1 \in \mathbb{Z}$. Suppose that $\gcd(c_0, d_0^2 + 1) = 1$ and $\gcd(c_1, d_1^2 + 1) = 1$. Suppose that there exist integers x_0 and x_1 such that $c_0x_0 + d_0 = c_1x_1 + d_1$. Then the integer values of the polynomial $(c_0c_1x + c_0x_0 + d_0)^2 + 1$ are coprime.*

Proof. (a) If p is a prime which divides all the integer values of $(cx + d)^2 + 1$, then p divides $d^2 + 1$, $c(c+2d)$ and $c(c-2d)$. Hence, if p does not divide c, then p divides $c+2d$ and $c-2d$, and thus divides $4d$. It follows that $p = 2$. But this is a contradiction, since then c is odd, and then $c^2 + 2d$ is also odd. Thus p divides $\gcd(c, d^2 + 1)$. Reciprocally, if the values of $(cx + d)^2 + 1$ are coprime, then $d^2 + 1$ and $c(c + 2d)$ are coprime and, hence, $d^2 + 1$ and c are coprime, as desired.

(b) In view of part (a), it suffices to prove that $gcd((c_0x_0 + d_0)^2 + 1, c_0c_1) = 1$. □

Remark 2.3.6. The two lines used in the proof of Proposition 2.3.4 are far from unique, and many other such lines could have been used. In fact, we believe that there are infinitely many propagating 2-cycles P on V_2 such that the second line passing through P in reduced integer parametrisation with $b_2(t) = b_0 + \lambda_2 t$ is such that $\gcd(b_0^2 + 1, \lambda_2) = 1$.

To speed up the verification of Theorem 2.1.4, we created in advance a set of about 150 different second lines in reduced integer parametrisation with $\gcd(b_0^2 + 1, \lambda_2) = 1$, and computed all bases $b \leq 10^6$ such that $b^2 + 1$ is prime and such that $S_{x^2,b}$ has a known 2-cycle on one of our 150 such lines. To eliminate such a b from $L(x^2, 2)$ required then to produce only one cycle of length greater than 2 for $S_{x^2,b}$, which is a very quick computation.

Example 2.3.7. Consider $b_0 := 288504$, an unusual base discovered when verifying Theorem 2.1.5. In this case, S_{x^2,b_0} has exactly 104 distinct cycles, all of them of length at most 7. All non-trivial cycles are

propagating, with forty-seven 1-cycles, thirty-nine 2-cycles, ten 3-cycles, six 5-cycles, and one cycle of length $4, 6$, and 7, respectively.

To illustrate propagation, note that the very first base $b > 2$ to have a 7-cycle is $b = 15$, with $c := \mathrm{cyc}(50, 34, 20, 26, 122, 68, 80)$ (see [HP78], page 10).[1] The reduced integer parametrisation of the line passing through this 7-cycle starts with $b(t) = 113t + 15$, $x_1(t) = 36t + 5$, $y_1(t) = 25t + 3$, etc. We find that when $\mathbf{t} = 2553$, the corresponding integer point on the line produces the 7-cycle for $b(\mathbf{t}) = 288504$ found in our search.

All cycles of length at least 2 are found among the orbits of n with $1 \leq n \leq 1,964,329,269$. Among the thirty-nine propagating 2-cycles, one of them, $\mathrm{cyc}(36253850477, 38091031810)$ is such that the second line associated to it has $\gcd(b_0^2 + 1, \lambda_2) = 1$ when written in reduced integer parametrisation.

2.4 1-cycles of $S_{x^2,b}$

In this section, we complement Subramanian's Theorem 2.1.3 with Proposition 2.4.1, and further study the surface V_1 associated with 1-cycles when $\phi(x) = x^2$.

Proposition 2.4.1. *Let $n := x + by$ be a non-trivial 1-cycle for $S_{x^2,b}$, and let $d := \gcd(b^2 + 1, n)$. Then $d > 1$, and there exists another 1-cycle $N := x + b(b - y)$ for $S_{x^2,b}$ such that, letting $D := \gcd(b^2 + 1, N)$, we have $D > 1$ and $b^2 + 1 = dD$.*

Let now $g := \gcd(x, y)$, $g' := \gcd(x, b - y)$, $h := \gcd(x - 1, y)$, and $h' := \gcd(x - 1, b - y)$. Then

(a) *$x = gg'$, $y = gh$, $b - y = g'h'$, and $x - 1 = hh'$.*

(b) *$d = n/g^2$, and $D = N/g'^2$.*

Proof. We leave it to the reader to check that N is a non-trivial 1-cycle. By hypothesis, $x(x-1) = y(b-y)$. Since x and $x - 1$ are coprime, we find that $y = gh$ and $b - y = g'h'$. Then $x(x - 1) = (gg')(hh')$. By

[1] Note a typo in [HP78] in the list of cycles for $b = 15$: the cycle just before c should be the non-propagating 5-cycle $\mathrm{cyc}(41, 125, 89, 221, 317)$.

definition, again since x and $x-1$ are coprime, we find that gg' is coprime to $x-1$, and it follows that gg' divides x. The same argument shows that hh' divides $x-1$. The equality $x(x-1)=(gg')(hh')$ implies then that $gg'=x$ and $hh'=x-1$, proving Part (a).

We claim that $d>1$. Indeed, if $d=1$, then $n=x+by$ divides $x+by-y^2$ and, hence, divides y^2. This is a contradiction since $0<y^2<x+by$. Similarly, $D>1$ since otherwise N divides $x+by-y^2$, which is also a contradiction since $N>x+by-y^2$. The reader will check directly that

$$nN=(b^2+1)(x+by-y^2)=(b^2+1)x^2.$$

Note that it follows from this equality that $n\neq N$, since otherwise b^2+1 would be a square, which is not possible since $b>0$. Using Part (a) and this equality, we find that

$$(n/g^2)(N/g'^2)=b^2+1.$$

It is then clear from this latter equality that (n/g^2) divides d, and that (N/g'^2) divides D. To finish the proof of Part (b), it suffices to prove that $dD=b^2+1$.

For this, it suffices to show that for every prime p, we have $\mathrm{ord}_p(dD)=\mathrm{ord}_p(b^2+1)$. First, note that dD and b^2+1 have the same prime divisors. Indeed, it is clear from the definitions that if p divides either d or D, then it divides b^2+1. On the other hand, if p divides b^2+1, then it divides nN and, hence, it divides d or D.

Let us show now that for every prime p, $\mathrm{ord}_p(dD)\leq\mathrm{ord}_p(b^2+1)$. The inequality is clear if either $\alpha:=\mathrm{ord}_p(d)=0$ or $\beta:=\mathrm{ord}_p(D)=0$, so we may assume that $\alpha,\beta>0$. Then $p^\alpha\cdot p^\beta$ divides nN and since $nN=(b^2+1)x^2$, we obtained the desired inequality if we show that p does not divide x. Assume by contradiction that p divides x. Since by hypothesis, p also divides $n=x+by$, we find that p divides by and, hence, p divides y because p cannot divide b since it divides b^2+1. Again by hypothesis, p divides N, so p divides $N-x+by=b^2$, which is impossible. As a result, p does not divide x.

We now show that for every prime p, $\mathrm{ord}_p(dD) \geq \mathrm{ord}_p(b^2+1)$. Let $\gamma := \mathrm{ord}_p(b^2+1) > 0$, and assume by contradiction that $\gamma > \alpha + \beta$. Then $\gamma > \alpha$ and $\gamma > \beta$, which by definition implies that $\alpha = \mathrm{ord}_p(n)$ and $\beta = \mathrm{ord}_p(N)$. This is a contradiction, since we can conclude from $(b^2+1)x^2 = nN$ that $\gamma \leq \mathrm{ord}_p(nN) = \alpha + \beta$. □

Proposition 2.4.2. *Recall the surface V_1 in $\mathbb{A}^3$ given by the equation $x^2 + y^2 - (x + by) = 0$. Given any point $P := (b_0, x_0, y_0)$ on V_1 outside of the lines $(t, 0, 0)$ and $(t, 1, 0)$, there exist exactly two lines in $\mathbb{A}^3$ that are entirely contained in V_1 and pass through P, namely the two lines given by the parametric equations*

$$\begin{aligned} &b(t) := b_0 + t((x_0-1)^2 + y_0^2), \quad x(t) := x_0 + t(x_0-1)y_0, \quad y(t) := y_0 + ty_0^2, \\ &b(t) := b_0 + t(x_0^2 + y_0^2), \qquad\qquad x(t) := x_0 + tx_0y_0, \qquad\qquad y(t) := y_0 + ty_0^2. \end{aligned}$$

The first parametric equation parametrises the same line through P as the line given in Theorem 2.2.4. *Let $d := \gcd(b_0^2+1, x_0 + b_0y_0)$, and $D := (b_0^2+1)/d$. In reduced integer form, the first line has $b(t) = b_0 + Dt$ and the second line has $b(t) = b_0 + dt$.*

Proof. It is straightforward to check that the two lines described in the proposition lie on the surface V_1. The equations for these two lines were found using the same method as in the proof of Proposition 2.3.1, and this method shows that exactly two lines through P exist. Recall that the line in Theorem 2.2.4 is given by the parametric equations

$$B(t) = b_0 + (b_0^2+1)t, \quad X(t) = x_0 + (x_0b_0 - y_0)t, \quad Y(t) = y_0 + (x_0 + b_0y_0)t.$$

To see that it equals the first line of the proposition, we make the change of variable $t = (b_0^2+1)s$ in the first line, and $t = ((x_0-1)^2 + y_0^2)s$ in the other line, so that $b((b_0^2+1)s) = B(((x_0-1)^2 + y_0^2)s)$. It remains to note that

$$\begin{aligned} \tfrac{x((b_0^2+1)s)-x_0}{s} &= (x_0-1)y_0(b_0^2+1) \\ &= (x_0b_0 - y_0)((x_0-1)^2 + y_0^2) \quad = \tfrac{X(((x_0-1)^2+y_0^2)s)-x_0}{s}, \end{aligned}$$

and

$$\begin{aligned}\tfrac{y((b_0^2+1)s)-y_0}{s} &= y_0^2(b_0^2+1)\\ &= (x_0+b_0y_0)((x_0-1)^2+y_0^2) \quad = \tfrac{Y(((x_0-1)^2+y_0^2)s)-y_0}{s}.\end{aligned}$$

□

2.5 Short Cycles of $S_{x^3,b}$

In this section, $\phi(x) = x^3$. We exhibit below several parametric families of 1-cycles for $S_{x^3,b}$. After we became aware of [DJ82], we noted that most of Proposition 2.5.1 already appears as Theorems 2-5 in [DJ82]. Only parts (c) and (d) in Proposition 2.5.1 are in slightly stronger form than in [DJ82].

Proposition 2.5.1. *Let $k \geq 1$ be a positive integer.*

(a) *Let $b = 3k+1$. Then $n := [2k+1, 0, k+1]_b$, $n := [0, 2k+1, k]_b$, and $n := [1, 2k+1, k]_b$ are 1-cycles for $S_{x^3,b}$.*

(b) *Let $b = 3k+2$. Then $n := [2k+1, 0, k]_b$ is a 1-cycle for $S_{x^3,b}$.*

(c) *Let $b = 9k+3$. Then $n := [6k+2, 4k+2, 5k+1]_b$ is a 1-cycle for $S_{x^3,b}$.*

(d) *Let $b = 9k+6$. Then $n := [6k+4, 2k+1, 7k+5]_b$ is a 1-cycle for $S_{x^3,b}$.*

Proof. An integer $n := [x, y, z]_b$ is a 1-cycle for $S_{x^3,b}$ if and only if the equation

$$x^3 + y^3 + z^3 = x + yb + zb^2$$

is satisfied. That this is the case can be checked directly. □

Remark 2.5.2. There are bases b of the form $b = 9k$, such as $b = 72$, 90, or 270, for which $S_{x^3,b}$ does not have any non-trivial 1-cycle. The bases $b = 18, 27$, and 54 have exactly one non-trivial 1-cycle, and $b = 108$ and 153 have exactly one non-trivial 1-cycle, which has 4 digits when written in base b (note it follows from Theorem 2.1.2 that a 1-cycle $[n]$ for $S_{x^3,b}$ is such that n has at most 4 digits in base b).

Thus Proposition 2.5.1 cannot immediately be generalised to include the case where $b = 9k$. But when $b = 9k^2$, Proposition 2.5.4 shows that $S_{x^3,b}$ has at least six non-trivial 1-cycles. When 9 divides b, we have only succeeded in producing parametric families of 1-cycles where b is a quadratic function of k, as in our next proposition.

Proposition 2.5.3. *Let $b = 9(730k^2 - 1)$. Then $n := [27k, 3k]_b = 730(3k)^3$ is a 1-cycle for $S_{x^3,b}$.*

Proof. An integer $n := [x, y]_b$ is a 1-cycle for $S_{x^3,b}$ if and only if the equation $x^3 + y^3 = x + yb$ is satisfied. Looking at this equation in the form $x(x-1)(x+1) = y(b-y^2)$, we can impose that y divide one of the factors x, $x+1$, or $x-1$, and solve for $b := y^2 + x(x-1)(x+1)/y$. If we want for 9 to divide b, we need to impose that $y = 3k$, and when we impose that y divide x, we can take for instance $x = 27k$, leading to the statement of the proposition. □

Proposition 2.5.4. *Let $k \geq 2$ be a positive integer.*

(a) *Suppose that $b = k^2$. Then $[0, k]_b$ and $[1, k]_b$ are 1-cycles for $S_{x^3,b}$.*

(b) *Suppose that $b = (3k+1)^2$. Then $[2k+1, k+1]_b$ is a 1-cycle for $S_{x^3,b}$.*

(c) *Suppose that $b = (3k+2)^2$. Then $[2k+1, k]_b$ is a 1-cycle for $S_{x^3,b}$.*

(d) *Suppose that $b = (3k)^2$. Then $[0, 6k^2+k, 3k^2+2k]_b$, $[1, 6k^2+k, 3k^2+2k]_b$, $[0, 6k^2-k, 3k^2-2k]_b$ and $[1, 6k^2-k, 3k^2-2k]_b$ are 1-cycles for $S_{x^3,b}$.*

Proof. An integer $n := [x, y]_b$ is a 1-cycle for $S_{x^3,b}$ if and only if the equation $x^3 + y^3 = x + yb$ is satisfied. That this is the case can be checked directly. Similarly, for (d), an integer $n := [x, y, z]_b$ is a 1-cycle for $S_{x^3,b}$ if and only if the equation $x^3 + y^3 + z^3 = x + yb + zb^2$ is satisfied. □

Remark 2.5.5. When $\phi(x) = x^2$ and x^3, the set of bases b such that $S_{\phi,b}$ has a 1-cycle has positive lower density (see Theorem 2.1.3 and Proposition 2.5.1). We do not know if this remains the case when $\phi(x) = x^m$ and $m \geq 4$.

When $\phi(x) = x^m$ with $m \geq 3$, we only found the following parametric families, which show that the sets of integer values of certain polynomials $f(t)$ of degree $m-1$ are contained in the set of bases b where

$S_{x^m,b}$ has a 1-cycle. When $b = c^{m-1}$, then $[c^m]$ and $[1 + c^m]$ are 1-cycles for $S_{\phi,b}$. When $b = 2c^{m-1} - 1$, then $[c + bc]$ is a 1-cycle. When $b = c\frac{c^{m-1}-1}{c-1} + (c-1)^{m-1}$, then $[c + b(c-1)]$ is a 1-cycle. When m is odd, and $b = c\frac{c^{m-1}-1}{c+1} + (c+1)^{m-1}$, then $[c + b(c+1)]$ is a 1-cycle.

When $m = 3$, the parametrisations above produce 1-cycles when $b = 2c^2 - 1$, $2c^2 - c + 1$, and $2c^2 + c + 1$. Unfortunately, none of these values of b are divisible by 3.

Remark 2.5.6. Let $W_1/\mathbb{Q}$ denote the algebraic surface defined by the equation $x^3 + y^3 - (x + by) = 0$ in the affine space $\mathbb{A}^3$. General results on singular cubic surfaces in $\mathbb{A}^3$ predict that W_1 can contain at most 15 lines of $\mathbb{A}^3$ (use [BW79], Lemma 3 (c) and [BW79, page 255]). Unfortunately, none of these lines produces non-trivial 1-cycles for $S_{x^3,b}$.

Let $W_1'/\mathbb{Q}$ denote the algebraic surface defined by the equation $x^3 + y^3 - (x + b^2y) = 0$ in the affine space $\mathbb{A}^3$. The associated projective cubic surface in $\mathbb{P}^3$ is non-singular, and thus contains 27 lines of $\mathbb{P}^3$ (over $\mathbb{C}$). Some of these lines produce the parametrisations in Proposition 2.5.4 (b), (c), and (d).

Let us now consider 2-cycles of $S_{x^3,b}$. As noted already in Example 2.2.2, we have the following parametric family: when $b = c^4$, then $\mathrm{cyc}(c^3, c^9)$ is a 2-cycle for $S_{x^3,b}$, and in this example, one of the integer in the cycle is a 3-digit number in base b, since $c^9 = [0, 0, c]_b$. Using this example, we find that every value of the polynomial $f(t) = t^4$ is among the bases b such that $S_{x^3,b}$ has a 2-cycle. The following proposition allows us to prove the same statement with a quadratic polynomial $f(t)$.

Proposition 2.5.7. *Let W denote the algebraic variety in $\mathbb{A}^5$ defined by the equations $x^3+y^3 = u+bv$ and $u^3 + v^3 = x + by$. The variety W contains the following two rational curves given by the parametrisations*

$$\begin{aligned}
&b(t) := 9t^2 + 15t + 7, \quad x(t) := 2t + 2, \quad y(t) := t, \qquad u(t) := t, \qquad v(t) := t + 1,\\
&b(t) := 9t^2 + 21t + 13, \quad x(t) := 2t + 3, \quad y(t) := t + 1, \quad u(t) := t + 1, \quad v(t) := t + 2.
\end{aligned}$$

For every integer $\mathbf{t} \geq 0$, $\mathrm{cyc}(n(\mathbf{t}), m(\mathbf{t}))$ is a 2-cycle for $S_{x^3,b(\mathbf{t})}$, where $n(\mathbf{t}) := x(\mathbf{t}) + y(\mathbf{t})b(\mathbf{t})$ and $m(\mathbf{t}) := u(\mathbf{t}) + v(\mathbf{t})b(\mathbf{t})$.

Proof. It is straightforward to verify that $(b(t), x(t), y(t), u(t), v(t))$ verifies the equations of W in both cases. It is also clear that $0 \leq x(\mathbf{t}), y(\mathbf{t}), u(\mathbf{t}), v(\mathbf{t}) < b(\mathbf{t})$. □

Note that $b(t) - 1$ factorises for both parametrisations, as $(3t + 2)(3t + 3)$ and $(3t + 3)(3t + 4)$, respectively. Thus for any integer $\mathbf{t}$, $b(\mathbf{t})$ is of the form $n(n + 1) + 1$ with either n or $n + 1$ divisible by 3.

2.6 A Lower Bound on the Number of Distinct Cycles of $S_{x^m,b}$

In this section, we slightly generalise Theorem 12 of H. Grundman and E. Teeple in [GT01] from the case $\phi(x) = x^3$ to $\phi(x) = x^m$ for all $m \geq 3$. Given positive integers m and b, define

$$N = N(m, b) := \prod_{\substack{p \text{ prime} \\ p-1 \mid (m-1) \\ p \leq b-1}} p \quad \cdot \prod_{\substack{p \text{ prime} \\ p^{r-1}(p-1) \mid (m-1) \\ p > b-1 \\ \operatorname{ord}_p(m-1) = r-1}} p^r.$$

Proposition 2.6.1. *Let $\phi(x) = x^m$ with $m \geq 2$. Let $b \geq 2$. Then $S_{x^m,b}$ has at least $\gcd(b - 1, N)$ distinct cycles. In particular, when $m \geq 5$ is prime and $b = mk + 1$, then $S_{x^m,b}$ has at least m distinct cycles.*

To prove Proposition 2.6.1, we use the following slightly more general set-up.

Proposition 2.6.2. *Let $b \geq 2$ and set $B := \{0, 1, \ldots, b - 1\}$. Let $\phi : B \to \mathbb{Z}_{\geq 0}$. Suppose that there exists a positive integer ℓ such that $\ell \mid b - 1$ and such that $\phi(n) \equiv n \pmod{\ell}$ for all $n \in B$. Then*

$$S_{\phi,b}(n) \equiv n \pmod{\ell} \text{ for all } n \in \mathbb{Z}_{\geq 0}.$$

In particular, the cycles associated to the orbits of $n \in \{1, \ldots, \ell\}$ under $S_{\phi,b}$ are all pairwise distinct, so that $S_{\phi,b}$ has at least ℓ distinct cycles.

Proof. Write $n = \sum_{i=0}^{d} n_i b^i$ in base b. Then

$$S_{\phi,b}(n) = \sum_{i=0}^{d} \phi(n_i) \equiv \sum_{i=0}^{d} n_i \equiv \sum_{i=0}^{d} n_i b^i = n \pmod{\ell}.$$

It follows that the cycles associated to the orbits of $n \in \{1, \ldots, \ell\}$ under $S_{\phi,b}$ are all pairwise distinct. □

Proof of Proposition 2.6.1. Suppose that p is a prime such that $p-1$ divides $m-1$. Then for all $n \in \mathbb{Z}$, $n^m \equiv n \pmod{p}$. Suppose now that $p > b-1$ and that $\varphi(p^r) = p^{r-1}(p-1)$ divides $m-1$. Then the class of every integer $n \leq p-1$ is a unit in $\mathbb{Z}/p^r\mathbb{Z}$, and so by Euler's Theorem, $n^m \equiv n \pmod{p^r}$. It follows that $N(m,b)$ divides $n^m - n$ for all integers in B, and we can apply Proposition 2.6.2 with $\ell = N(m,b)$. □

Corollary 2.6.3. *Let $\phi(x) = x^3$. Let k be any positive integer and set $b = 3k+1$. Then $S_{x^3,b}$ has at least 5 distinct cycles.*

Proof. We know that $[1]$ is a cycle. Using Proposition 2.6.2, we obtain that the orbit of $n = 3$ produces a cycle consisting entirely of integers congruent to 0 modulo 3. Proposition 2.5.1 (a) exhibits three non-trivial cycles consisting of integers congruent to 1 or 2 modulo 3. □

Bibliography

[AM57] A. A. Albert and B. Muckenhoupt. "On matrices of trace zeros". In: *Michigan Math. J.* 4 (1957), pp. 1–3.

[App98] G. D. Appleby. "Similarity classes for nilpotent operators over Dedekind domains". In: *Linear Algebra Appl.* 274 (1998), pp. 37–59.

[Bar85] R. Barlow. "Rational equivalence of zero cycles for some more surfaces with $p_g = 0$". In: *Invent. Math.* 79.2 (1985), pp. 303–308.

[Bau14] I. Bauer. "Bloch's conjecture for Inoue surfaces with $p_g = 0$, $K^2 = 7$". In: *Proc. Amer. Math. Soc.* 142.10 (2014), pp. 3335–3342.

[Bau+12] I. Bauer, F. Catanese, F. Grunewald, and R. Pignatelli. "Quotients of products of curves, new surfaces with $p_g = 0$ and their fundamental groups". In: *Amer. J. Math.* 134.4 (2012), pp. 993–1049.

[BF15] I. Bauer and D. Frapporti. "Bloch's conjecture for generalized Burniat type surfaces with $p_g = 0$". In: *Rend. Circ. Mat. Palermo (2)* 64.1 (2015), pp. 27–42.

[Bha03] S. M. Bhatwadekar. "A cancellation theorem for projective modules over affine algebras over C_1-fields". In: *J. Pure Appl. Algebra* 183.1-3 (2003), pp. 17–26.

[BKL76] S. Bloch, A. Kas, and D. Lieberman. "Zero cycles on surfaces with $p_g = 0$". In: *Compositio Math.* 33.2 (1976), pp. 135–145.

[Blo10] S. Bloch. *Lectures on algebraic cycles*. 2nd ed. Vol. 16. New Mathematical Monographs. Cambridge University Press, Cambridge, 2010.

[BDG80] M. Boratyński, E. D. Davis, and A. V. Geramita. "Complete decomposability in the exterior algebra of a free module". In: *Canadian J. Math.* 32.1 (1980), pp. 27–33.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[Bou57] V. Bouniakowsky. "Sur les diviseurs numériques invariables des fonctions rationnelles entières". In: *Mém. Acad. Sc. St. Pétersbourg.* 6 (1857), pp. 305–329.

[Bro+90] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith. "A new table of constant weight codes". In: *IEEE Trans. Inform. Theory* 36.6 (1990), pp. 1334–1380.

[BW79] J. W. Bruce and C. T. C. Wall. "On the classification of cubic surfaces". In: *J. London Math. Soc. (2)* 19.2 (1979), pp. 245–256.

[Cla18] P. L. Clark. "A note on rings of finite rank". In: *Comm. Algebra* 46.10 (2018), pp. 4223–4232.

[DG77] E. D. Davis and A. V. Geramita. "Efficient generation of maximal ideals in polynomial rings". In: *Trans. Amer. Math. Soc.* 231.2 (1977), pp. 497–505.

[DJ82] L. E. Deimel Jr. and M. T. Jones. "Finding pluperfect digital invariants: techniques, results and observations". In: *J. Recreational Math.* 14.2 (1981/82), pp. 87–108.

[DF04] D. S. Dummit and R. M. Foote. *Abstract algebra*. 3rd ed. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[EM80] D. R. Estes and J. R. Matijevic. "Local-global criteria for outer product rings". In: *Canadian J. Math.* 32.6 (1980), pp. 1353–1360.

[FS01] L. Fuchs and L. Salce. *Modules over non-Noetherian domains*. Vol. 84. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2001.

[Gen17] J. E. Gentle. *Matrix algebra: Theory, Computations and Applications in Statistics*. 2nd ed. Springer Texts in Statistics. Springer, Cham, 2017.

[GT01] H. G. Grundman and E. A. Teeple. "Generalized happy numbers". In: *Fibonacci Quart.* 39.5 (2001), pp. 462–466.

[HL23] G. H. Hardy and J. E. Littlewood. "Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes". In: *Acta Math.* 44.1 (1923), pp. 1–70.

[Har77] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[HP78] H. Hasse and G. Prichett. "A conjecture on digital cycles". In: *J. Reine Angew. Math.* 298 (1978), pp. 8–15.

[HL07] W. J. Heinzer and L. S. Levy. "Domains of dimension 1 with infinitely many singular maximal ideals". In: *Rocky Mountain J. Math.* 37.1 (2007), pp. 203–214.

[Hin72] Y. Hinohara. "On semilocal OP-rings". In: *Proc. Amer. Math. Soc.* 32 (1972), pp. 16–20.

[IM79] H. Inose and M. Mizukami. "Rational equivalence of 0-cycles on some surfaces of general type with $p_g = 0$". In: *Math. Ann.* 244.3 (1979), pp. 205–217.

[Iwa78] H. Iwaniec. "Almost-primes represented by quadratic polynomials". In: *Invent. Math.* 47.2 (1978), pp. 171–188.

[JW17] J. R. Juett and J. L. Williams. "Strongly stable rank and applications to matrix completion". In: *Comm. Algebra* 45.9 (2017), pp. 3967–3985.

[Kap74] I. Kaplansky. *Commutative rings*. Revised ed. The University of Chicago Press, Chicago, Ill.-London, 1974.

[KS02] A. Krishna and V. Srinivas. "Zero-cycles and K-theory on normal surfaces". In: *Ann. of Math. (2)* 156.1 (2002), pp. 155–195.

[KS07] A. Krishna and V. Srinivas. "Zero cycles on singular varieties". In: *Algebraic cycles and motives. Vol. 1*. Vol. 343. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2007, pp. 264–277.

[KS10] A. Krishna and V. Srinivas. "Zero cycles on singular affine varieties". In: *Cycles, motives and Shimura varieties*. Vol. 21. Tata Inst. Fund. Res. Stud. Math. Tata Inst. Fund. Res., Mumbai, 2010, pp. 243–264.

[LR94] T. J. Laffey and R. Reams. "Integral similarity and commutators of integral matrices". In: *Linear Algebra Appl.* 197/198 (1994). Second Conference of the International Linear Algebra Society (ILAS) (Lisbon, 1992), pp. 671–689.

[Lan02] S. Lang. *Algebra*. 3rd ed. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.

[Lem12] R. J. Lemke Oliver. "Almost-primes represented by quadratic polynomials". In: *Acta Arith.* 151.3 (2012), pp. 241–261.

[Len77] H. W. Lenstra Jr. "Euclidean number fields of large degree". In: *Invent. Math.* 38.3 (1976/77), pp. 237–254.

[Lis61] D. Lissner. "Matrices over polynomial rings". In: *Trans. Amer. Math. Soc.* 98 (1961), pp. 285–305.

[Lis65] D. Lissner. "Outer product rings". In: *Trans. Amer. Math. Soc.* 116 (1965), pp. 526–535.

[Lor+20] D. Lorenzini, M. Melistas, A. Suresh, M. Suwama, and H. Wang. "Integer Dynamics". submitted. 2020. URL: http://alpha.math.uga.edu/~lorenz/Integer Dynamics.pdf.

[Mat89] H. Matsumura. *Commutative ring theory*. 2nd ed. Vol. 8. Cambridge Studies in Advanced Mathematics. Translated from the Japanese by M. Reid. Cambridge University Press, Cambridge, 1989.

[Mes06] Z. Mesyan. "Commutator rings". In: *Bull. Austral. Math. Soc.* 74.2 (2006), pp. 279–288.

[MMR88] N. Mohan Kumar, M. P. Murthy, and A. Roy. "A cancellation theorem for projective modules over finitely generated rings". In: *Algebraic geometry and commutative algebra, Vol. I*. Kinokuniya, Tokyo, 1988, pp. 281–287.

[MS76] M. P. Murthy and R. G. Swan. "Vector bundles over affine surfaces". In: *Invent. Math.* 36 (1976), pp. 125–165.

[OEIS] O. F. I. (2021). *The On-Line Encyclopedia of Integer Sequences*. URL: http://oeis.org/A161872.

[PW16] C. Pedrini and C. Weibel. "Some surfaces of general type for which Bloch's conjecture holds". In: *Recent advances in Hodge theory*. Vol. 427. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2016, pp. 308–329.

[RR00] M. Rosset and S. Rosset. "Elements of trace zero that are not commutators". In: *Comm. Algebra* 28.6 (2000), pp. 3059–3072.

[Sch66] J. Schönheim. "On maximal systems of k-tuples". In: *Studia Sci. Math. Hungar.* 1 (1966), pp. 363–368.

[Sho37] K. Shoda. "Einige Sätze über Matrizen". In: *Jpn. J. Math.* 13.3 (1937), pp. 361–365.

[SS03] M. Spieß and T. Szamuely. "On the Albanese map for smooth quasi-projective varieties". In: *Math. Ann.* 325.1 (2003), pp. 1–17.

[Stacks] T. Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`. 2018.

[Sta16] A. Stasinski. "Similarity and commutators of matrices over principal ideal rings". In: *Trans. Amer. Math. Soc.* 368.4 (2016), pp. 2333–2354.

[Sta18] A. Stasinski. "Commutators of trace zero matrices over principal ideal rings". In: *Israel J. Math.* 228.1 (2018), pp. 211–227.

[Ste60] B. M. Stewart. "Sums of functions of digits". In: *Canadian J. Math.* 12 (1960), pp. 374–389.

[Sub68] P. K. Subramanian. "On bases and cycles". In: *Math. Mag.* 41 (1968), pp. 117–123.

[Swa87] R. G. Swan. "Vector bundles, projective modules and the K-theory of spheres". In: *Algebraic topology and algebraic K-theory (Princeton, N.J., 1983)*. Vol. 113. Ann. of Math. Stud. Princeton Univ. Press, Princeton, NJ, 1987, pp. 432–522.

[Tow68] J. Towber. "Complete reducibility in exterior algebras over free modules". In: *J. Algebra* 10 (1968), pp. 299–309.

[Tow70] J. Towber. "Local rings with the outer product property". In: *Illinois J. Math.* 14 (1970), pp. 194–197.

[Voi14] C. Voisin. "Bloch's conjecture for Catanese and Barlow surfaces". In: *J. Differential Geom.* 97.1 (2014), pp. 149–175.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. 2nd ed. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[Wei13] C. A. Weibel. *The K-book*. Vol. 145. Graduate Studies in Mathematics. An introduction to algebraic K-theory. American Mathematical Society, Providence, RI, 2013.

[Wil11] W. Willis. "Bounds for the independence number of a graph". MA thesis. Virginia Commonwealth University, 2011.

[Yoh67] C. R. Yohe. "Triangular and diagonal forms for matrices over commutative noetherian rings". In: *J. Algebra* 6 (1967), pp. 335–368.

Appendix A

Julia Code for Integer Dynamics

In this appendix, we include the Julia code that was used to verify that the base $b = 481360$ has only 2 distinct cycles for Theorem 2.1.4. Initially, we used Magma for the computation, and for any other base less than one million, Magma was fast enough to finish the computation. However for $b = 481360$, Magma was too slow and so we picked Julia to improve the speed.

A.1 Code

```
# Check up to numCycles cycles
const numCycles=3;
const b = 481360;

# check a number d has been seen already
# seen is an array of arrays of sets
# number n = d1 + d2*b + d3*b^2 is stored as d1 in seen[d3+1][d2+1]
function isSeen(seen,d)
    return d[1] in seen[d[3]+1][d[2]+1];
end;

# add number d to seen
# seen is an array of arrays of sets
# number n = d1 + d2*b + d3*b^2 is stored as d1 in seen[d3+1][d2+1]
function addSeen!(seen,d)
    push!(seen[d[3]+1][d[2]+1], d[1])
end;

# Checks if max(d[1],d[2]) + min(d[1],d[2])*b + d[2]*b^2 is smaller than x+b*y
# Uses separate comparison for speed purpose
function isSmaller(d,x,y)
    return d[3] == 0 && (min(d[1],d[2]) < y ||
                (min(d[1],d[2])==y && max(d[1],d[2]) < x))
end
```

```
# start the sum of the square procedure until it hits a cycle or a number
# already seen
# Returns True if it finds a new cycle
function traverse(x,y,d,seen,cycles)
    # if the number already appeared then skip it
    if x in seen[1][y+1]
        return false
    end;
    n = x+b*y;

    L =[n];
    while !(isSeen(seen,d))
        addSeen!(seen,d)
        n = sum(i^2 for i in d);
        push!(L,n)
        digits!(d, n, base = b)
        # if d is less than x+b*y then we have seen it already
        if isSmaller(d, x, y)
            return false
        end
    end
    # find the position of n in L
    p = findfirst(isequal(n), L);
    # if n is in L and not the last, then there is a cycle starting at
    # the first appearance of n
    if p != nothing && p < length(L)
        push!(cycles, L[p:length(L)-1])
        return true
    end
    return false
end

# Check all the numbers x+b*y with low<=y<=high
function checkYInterval(low, high, seen, cycles)
    for y=low:high
        for x=max(y,ceil(Int, sqrt(y*b-y^2+1/4)+1/2)):b-1
            d = [x, y, 0];
            if traverse(x, y, d, seen, cycles)
                # Stop if it finds enough cycles
                if length(cycles) >= numCycles
                    return nothing
                end
            end
        end
        # delete unncessary seen to save memory.
        seen[1][y+1] = Set{Bool}()
    end
end

# b is UInt32
# indexing is off by 1
# if n = [a,b,c] then check if a is in seen[c+1][b+1]
# keeps track of [a,b,c] where a>=b and c=0 or 1
seen = [[ Set{UInt32}() for i=1:b], [Set{UInt32}() for i=1:b]];
cycles = [[1]];
push!(seen[1][1],1);

checkYInterval(0, b-1, seen, cycles);
println(cycles)
```

A.2 Explanation of the Code

In this section, we explain the Julia code included in Section A.1.

A.2.1 Preliminaries

Let $B := \{0, 1, \ldots, b^3 - 1\}$, and for $x, y, z \in \mathbb{Z}$, let $[x, y, z]_b$ denote $x + yb + zb^2$. Let $f_b : B \to B$ be a map where $f_b([x, y, z]_b) = [\max(x, y), \min(x, y), z]_b$, and $\leq_b$ an ordering where

$$[x_0, x_1, x_2]_b \leq_b [y_0, y_1, y_2]_b \iff f_b([x_0, x_1, x_2]_b) \leq f_b([y_0, y_1, y_2]_b).$$

Now suppose $\{n_1, \ldots, n_k\}$ is a cycle of length k. By Theorem 2.1.2, one of the n_i's has at most two digits. Applying S_{x^2} to a two digit n results in $[x, y, z]$ with $z = 0$ and 1, and further applying S_{x^2} preserves the property of z being either 0 or 1, so every n_i's have at most 3 digits with $z = 0$ or 1. Hence the ordering $\leq_b$ makes sense on $\{n_1, \ldots, n_k\}$ and so without loss of generality, assume n_1 is minimal with respect to $\leq_b$. Note that n_1 will have two digits since it is the smallest element. Now let $n_1 = [u, v, 0]_b$, and $x_0 = \max(u, v)$ and $y_0 = \min(u, v)$.

A.2.2 The bound on the for loop on line 60

Here we explain the lower bound on x in line 60. First, we have $[u, v, 0]_b = n_1 \leq_b n_2 = u^2 + v^2 = x_0^2 + y_0^2$ by the minimality of n_1, and since $f_b(n) \leq n$, we have

$$x_0 + by_0 = [x_0, y_0, 0] = f_b([u, v, 0]) \leq f_b(n_2) \leq n_2 = x_0^2 + y_0^2.$$

From $x_0 + by_0 \leq x_0^2 + y_0^2$, we have

$$\tfrac{1}{2} + \sqrt{y_0(b - y_0) + \tfrac{1}{4}} \leq x_0.$$

Now notice that $S_{x^2}([u,v,0]_b) = S_{x^2}([x_0,y_0,0]_b)$, so $[x,y,0]_b$ will be a preperodic element. So to find all the cycles, it suffices to check all the numbers $[x,y,0]_b$ with $y \leq x$ and $\frac{1}{2} + \sqrt{y(b-y)+\frac{1}{4}} \leq x$. Hence on line 60, we are iterating through all x's satisfying

$$x \geq \max(y, \tfrac{1}{2} + \sqrt{y(b-y)+\tfrac{1}{4}}).$$

A.2.3 Detecting a cycle at lines 47 and 50

Suppose we are at line 47. Then we are looking for the position of the first n in the sequence L starting at $[x,y,0]_b$. Since we added n to L at line 39, there are two possible cases.

The first case is when n is the last element in L. This happens when we have seen n already starting at some other number $[x',y',0]_b <_b [x,y,0]_b$. In this case we can ignore this since it has already been checked. This is the case $p = \text{length}(L)$ in line 50.

The second case is when the n is not the last element. Then the subsequence of L starting at the first n and ending before the last element in L is a cycle since the last element of L is n. So we add this cycle and return true from the function `traverse`.

A.2.4 Exiting at line 42

Suppose $d = [x',y',z'] <_b [x,y,0]$ and we exited the function `traverse` at line 42. We have already checked numbers $<_b [x,y,0]$ through the for loops on lines 59 and 60, so we may safely ignore d in this case and exit the function.