Calculating Ways to Calculate

by

Lars van der Kuil

To obtain the degree of Bachelor of Science
at the Delft University of Technology,
To be defended publicly on July 6 2023 at 13:30.

Student number:	5337402	
Project duration:	April 24, 2023 – July 6, 2023	
Thesis committee:	Dr. N.D. (Nikolaas) Verhulst,	TU Delft, supervisor
	Dr. ir. W.G.M. (Wolter) Groenevelt	TU Delft

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft

Summary

Algebras are vector spaces with a bilinear product. When we fix a finite dimension n and a finite field K with q elements, there are a finite number of non-isomorphic algebras. Seeing as vector spaces are completely determined by the dimension and scalar field, the number of non-isomorphic algebras is the number of ways we can define a bilinear product of vectors. Exploiting the bilinearity of the product we can construct a surjection from vectors of n $n \times n$ matrices over K to non-isomorphic n-dimensional algebras over K. This function can be made injective by reducing to orbits under a group action on the set of vectors of matrices, thus providing a bijection. So the number of non-isomorphic algebras is equal to the number of orbits of this group action. In 2020 Verhulst [9] used Burnside's Lemma to count the orbits and thus the number of non-isomorphic algebras. However, the formula he derived still requires a number of complicated calculations.

The aim of this thesis is to implement Verhulst's formula in python. In Table 4.1 you can find the output of the python script. The results for $n = 1$ merely show some trivial cases. The results for $n = 2$ fit the formulas obtained, using completely different methods, by Petersson and Scherer [5]. The results for $n = 3$ and $n = 4$ are, to my knowledge, new. Currently, the limiting factor is computation time. A more powerful computer could squeeze out a few more results, but a more efficient formula is necessary. Based on the results, it seems that the contribution of the identity matrix in Verhulst's formula provides a decently tight lower bound.

Contents

1

Introduction

Linear algebra is a very powerful tool, but some vector spaces contain some additional multiplication structure. For instance, in the vector space of matrices we can multiply vectors using the matrix product and in $\mathbb{R}^3$ we can multiply vectors using the cross-product. This additional structure is described by an algebra - an extension of a vector space that adds a bilinear product.

The classification of finite-dimensional algebras is a hard problem, unlike in the case of vector spaces. In 1992, Althoen and Hansen [2] successfully classified 2-dimensional algebras over the base field $\mathbb{R}$. In 2000, Petersson [4] generalised this classification to arbitrary base fields, which Petersson and Scherer [5] used in 2004 to derive polynomial formulas in terms of q for the number of non-isomorphic 2-dimensional algebras over a finite field with q elements. Lastly, Verhulst [9] derived a formula for calculating the number of non-isomorphic n-dimensional algebras over a finite field in 2020.

However, this general formula is not entirely satisfactory as it requires a number of complex calculations, unlike the polynomial formulas developed by Petersson and Scherer. In this thesis, our goal is to implement Verhulst's formula in a Python program and collect data.

Chapter 2 will cover basic definitions and results concerning groups (Section 2.1), finite fields (Section 2.2), and vector spaces (Section 2.3). These concepts will be utilized in Chapter 3 to introduce the theory of algebras and in Chapter 4 to implement Verhulst's formula in a Python program, the results of which are also discussed in Chapter 4.

2

Preliminaries

In algebra, most definitions of structures are based on groups. Therefore, we will begin by reviewing the definition of a group, along with some fundamental properties and the concept of a group action. After that, we will delve into fields, followed by a well-known classification theorem for finite fields. Finally, we will define vector spaces over arbitrary fields.

2.1. Groups

A group is set with a single operation on it which satisfies some basic properties. These properties reflect the properties we commonly see in regular arithmetic.

Definition 2.1 (Group)**.** *A* group *is a pair* $(G, *)$ *of a set* G *and a binary operation,* $*$*, on* G *such that:*

- $\forall a, b \in G : a * b \in G$ *(closure)*
- $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ *(associativity)*
- $\exists e \in G : \forall a \in G : a * e = e * a = a$ *(*e *is the identity element)*
- $\forall a \in G : \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$ *(*a^{-1} *is the inverse of* a*)*

We call $(G, *)$ *an* Abelian *group if* $*$ *also satisfies:*

- $\forall a, b \in G : a * b = b * a$ *(commutativity)*

It is easy to check that the following are examples of groups.

Example 2.2. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ *are all Abelian groups.*

Example 2.3. *The set* $\mathrm{GL}_n(\mathbb{R})$ *of invertible* $n \times n$ *real matrices with matrix multiplication is a non-Abelian group.*

Note that all of these groups contain an infinite number of elements. A classic family of finite groups are the groups of modular arithmetic. Recall that we consider two numbers $a, b \in \mathbb{Z}$ to be congruent $\pmod{n}$ (write $a \equiv b \pmod{n}$) if and only if there exists a $k \in \mathbb{Z}$ such that $a = b + kn$. The relation $\equiv \pmod{n}$ is an equivalence relation. The set of equivalence classes with respect to this equivalence relation is $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$, where $\overline{a}$ is the equivalence class of $a \in \mathbb{Z}$.

Proposition 2.4. *For all $n \in \mathbb{N}$ we have that $\mathbb{Z}/n\mathbb{Z}$ with the operation $+$ given by $\overline{a}+\overline{b} = \overline{a+b}$ for $a, b \in \mathbb{Z}$ is an Abelian group.*

Proof. Cf. e.g. [7] p.13. □

In the next section, this group will play an important role in describing the finite fields.

For most concepts in mathematics there is some notion of 'essentially the same'. For groups, as for most algebraic objects, we call this notion isomorphism. The idea is that we map the elements of two groups to each other using a bijection, which respects the operations on the group.

Definition 2.5 (Group Isomorphism)**.** *Two groups $(G, *_G)$ and $(H, *_H)$ are said to be* isomorphic *($G \cong H$) if there exists a* group isomorphism *between G and H, that is, there exists a bijective function $\psi : G \to H$ such that for all $a, b \in G$ we have $\psi(a *_G b) = \psi(a) *_H \psi(b)$.*

Group actions describe symmetries and Burnside's Lemma is a very useful theorem for avoiding symmetries when counting. Suppose, for example, that we have 5 colours of beads and we want to know how many necklaces with 8 beads we can make. The simple answer would be 8^5, since each of the 8 beads can be one of 5 colours. However, two necklaces are essentially the same if they differ by a rotation or a reflection. These symmetries can be described using a group action, then we can use Burnside's Lemma to count the number of different necklaces.

Definition 2.6 (Group Action)**.** *Given a set X and a group G with identity element e, a (right)* G-action *on X is a map $\phi : X \times G \to X$ such that*

- $\forall x \in X : \phi(x, e) = x$
- $\forall x \in X, \forall g, h \in G : \phi(x, gh) = \phi(\phi(x, h), g)$

Example 2.7. *In the example of the necklace, we have a group consisting of rotations and reflections (see dihedral group in e.g. [7] p.68) acting on the set of all possible necklaces ignoring symmetries. The 'do nothing' element acts like doing nothing to any of the necklaces and is the identity in our group, so the first requirement is satisfied. If we apply a $\frac{2\pi}{5}$ rotation and then a $\frac{4\pi}{5}$ rotation to a necklace, then we have essentially rotated the necklace by a $\frac{6\pi}{5}$ rotation. So in our group the operation determines the net effect of the rotations and reflections. This also satisfies the second requirement.*

In this example we have found a group which, when acting on a necklace gives us an equivalent necklace. We say two elements, in this case necklaces, are in the same *orbit* if you can reach one from the other by applying the group action. More formally, for a G-action ϕ on X, we define the ϕ-orbit of an element $x \in X$ to be the set $G(x) = \{\phi(x, g) : g \in G\}$ and we write X/G for the set of ϕ-orbits.

Some actions do not have any effect on some necklaces while they do on others. A necklace with 5 beads all of the same colour does not change if it is rotated by $\frac{2\pi}{5}$. It does not just become an equivalent necklace, it becomes indistinguishable from the original, even in its position. We call this necklace a *fixpoint* of the $\frac{2\pi]}{5}$ rotation. Formally, we say that $X^g = \{x \in X : \phi(x, g) = x\}$ is the set of fixpoints of $g \in G$.

Burnside's Lemma uses the number of fixpoints of each group element to count the number of orbits under the group action, thereby counting the number of distinct necklaces. Application of this result to the necklace example will be left as an exercise for the reader.

Theorem 2.8 (Burnside's Lemma)**.** *Suppose ϕ is an action of a finite group G on a finite set X. Then*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

Proof. Cf. e.g. [7], p.58. □

For counting non-isomorphic algebras the symmetry lies in the isomorphism. In Chapter 3 we use a group-action to describe when two algebras are isomorphic.

2.2. Finite Fields

In essence, $\mathbb{R}$ is a set of objects which we can add, subtract, multiply and divide. We want to generalise this structure. This generalisation is captured in the following definition.

Definition 2.9 (Field)**.** *A* field *is a triple $(K,+,\cdot)$ of a set K and two binary operations, addition "$+$" and multiplication "$\cdot$", on K such that:*

- *$(K,+)$ is an Abelian group*
- *$(K\setminus\{0\},\cdot)$ is an Abelian group, where 0 is the identity element of $(K,+)$*
- *The distributive law holds: $\forall\alpha,\beta,\gamma\in K:(\alpha+\beta)\cdot\gamma=(\alpha\cdot\gamma)+(\beta\cdot\gamma)$*

If the operations on a field $(K,+,\cdot)$ are natural, already given or unimportant, then the field is referred to by just the set K. We write 0 when referring to the additive identity element of an arbitrary field K and similarly 1 for the multiplicative identity of K. Furthermore $-\alpha$ is the additive inverse of $\alpha\in K$ and α^{-1} or $\frac{1}{\alpha}$ is its multiplicative inverse. In some situations, the symbols for the operations are omitted: for $\alpha,\beta\in K$, $\alpha-\beta$ means $\alpha+(-\beta)$ and $\alpha\beta$ means $\alpha\cdot\beta$.

As mentioned before $\mathbb{R}$ with the usual addition and multiplication forms a field. It is not difficult to check that $\mathbb{Q}$ and $\mathbb{C}$ are also fields. Notably $\mathbb{Z}$ is not a field, since it does not contain e.g. $\frac{1}{2}$, the multiplicative inverse of $2\in\mathbb{Z}$.

Just like with groups, if fields are essentially the same we say they are isomorphic. Since our definition of a field is largely based on groups, our definition of a field-isomorphism will be similar to that of a group-isomorphism. In fact the definition given below is equivalent to saying that the underlying groups of the fields have to be isomorphic.

Definition 2.10 (Field Isomorphism)**.** *Two fields $(K,+_K,\cdot_K)$ and $(F,+_F,\cdot_F)$ are said to be* isomorphic *($K\cong F$) if there exists a* field isomorphism *between K and F, that is, there exists a bijective function $\psi:K\to F$ such that for all $\alpha,\beta\in K$ we have $\psi(\alpha+_K\beta)=\psi(\alpha)+_F\psi(\beta)$ and $\psi(\alpha\cdot_K\beta)=\psi(\alpha)\cdot_F\psi(\beta)$.*

Note that the examples of field mentioned earlier all contain an infinite number of elements. With the usual addition and multiplication this is unavoidable, since $a+1$ can never be a number smaller than or equal to a for any number a and a field must contain the identity elements 0 and 1. This is however not the case for modular arithmetic. In Proposition 2.4 we have seen that $\mathbb{Z}/n\mathbb{Z}$ is an Abelian group for all $n\in\mathbb{N}$. Similar to addition we multiply modulo n; for $\overline{a},\overline{b}\in\mathbb{Z}/n\mathbb{Z}$ we define $\overline{a}\cdot\overline{b}=\overline{a\cdot b}$. However this multiplication does not make $\mathbb{Z}/n\mathbb{Z}$ a field for all n. For example $(\mathbb{Z}/4\mathbb{Z})\setminus\{0\}$ is not closed under multiplication; $\overline{2}\cdot\overline{2}=\overline{4}=\overline{0}$. The following theorem shows exactly for which $n\in\mathbb{N}$ we have that $\mathbb{Z}/n\mathbb{Z}$ is a field.

Theorem 2.11. *$\mathbb{Z}/p\mathbb{Z}$ for $p \in \mathbb{N}$ is a field if and only if p is a prime number.*

Proof. Cf. e.g. [1] p.7. □

The fields $\mathbb{Z}/p\mathbb{Z}$ for p a prime number form the basis of all finite fields and are therefore known as prime fields.

Theorem 2.12 (Characterisation of the Finite Fields)**.** *For every prime number p and every positive integer k there exists, up to isomorphism, a unique field $\mathbb{F}_{p^k}$ containing p^k elements. Conversely, for every finite field K there exist a prime number p and a positive integer k such that $K \cong \mathbb{F}_{p^k}$.*

Proof. Cf. e.g. [1] p.126/127. □

This theorem motivates us to define *the* finite field with q elements $\mathbb{F}_q$ for any prime power q. Note that these fields are only defined up to isomorphism. Any sort of arithmetic happens in an instance of the finite field $\mathbb{F}_q$. For q a prime number we have already seen the prime fields $\mathbb{Z}/p\mathbb{Z}$. For q a higher power of a prime the field $\mathbb{F}_q$ can be constructed using polynomials. The details of this will not be important for the purposes of this thesis and we will thus refer to a book about field algebra like [1] (p.126/127). As an example we give a construction of $\mathbb{F}_4$.

Example 2.13. *The field of $4 = 2^2$ elements is the set $\mathbb{F}_4 = \{0, 1, X, X+1\}$ of polynomials with addition modulo 2 and multiplication given by*

·	0	1	X	X+1
0	0	0	0	0
1	0	1	X	X+1
X	0	X	X+1	1
X+1	0	X+1	1	X

2.3. Vector Spaces

Most people with a background in science will have seen vector spaces over $\mathbb{R}$. This definition can easily be generalised to vector spaces over an arbitrary field K. The difference is that scalars are no longer real numbers, but elements of the scalar field K.

Definition 2.14 (Vector Space)**.** *A* vector space *over a field K is an Abelian group $(V, +)$ with a left $(K \setminus \{0\}, \cdot)$-action $\cdot$ such that for all $\alpha, \beta \in K$, $u, v \in V$*

- $(\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u)$
- $\alpha \cdot (u + v) = (\alpha \cdot u) + (\alpha \cdot v)$

Most, if not all, theorems, definitions and methods generalise directly to vector spaces over arbitrary fields. The details will not be important for this thesis, so we will refer to an advanced linear algebra book (like [6]) for those. The following definitions and results will be essential for the rest of this thesis.

Definition 2.15 (Linear Function)**.** *Given two vector spaces V and W over a field K, a function $f : V \to W$ is called* linear *if for all $u, v \in V$, $\alpha, \beta \in K$ we have $f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$.*

For the definition of an algebra in Chapter 3 we will need a related concept, namely *bi*linear functions.

Definition 2.16 (Bilinear Function)**.** *Given three vector spaces V, V' and W over a field K, a function $f : V \times V' \to W$ is called* bilinear *if f is linear in both components, that is, $\forall v \in V' : u \mapsto f(u, v)$ and $\forall u \in V : v \mapsto f(u, v)$ are linear functions.*

Linear functions preserve the operations on a vector space. This motivates the following definition.

Definition 2.17 (Vector Space Isomorphism)**.** *Two vector spaces V and W are said to be* isomorphic *($V \cong W$) if there exists a* linear bijection *between V and W.*

Let K^n be the vector space of ordered sets with n components and elements in K. Addition and scalar multiplication on K^n are component-wise. Given a basis of an n-dimensional vector space V there is a unique way of writing the vectors of V as a linear combination of basis vectors. This leads to a linear bijection to K^n.

Proposition 2.18. *For any integer $n \in \mathbb{Z}_{\geq 1}$ and any field K there is, up to isomorphism, exactly one n-dimensional vector space over K.*

Proof. Let V be an n-dimensional vector space over K. Then by choosing a basis for V we can map the vectors of V to their coordinate vectors in K^n. So we map $v = \sum_{i=1}^{n} \alpha_i e_i$ to $(\alpha_1, \cdots, \alpha_n)$. This map is well-defined because of linear independence of the basis, linear because the summation is linear and bijective because span of the basis is the whole space V. So $V \cong K^n$. □

The image of a $v \in V$ under the isomorphism corresponding to a basis $\mathscr{B}$ is known as the coordinate vector of v and is denoted as $[v]_{\mathscr{B}}$. The idea of using a basis to change vectors to columns of field elements can also be used to change linear functions to matrices.

Theorem 2.19. *Let V and W be two vector spaces over a field K with dimensions n and m and bases $\mathscr{B}_V$ and $\mathscr{B}_W$ respectively. Then for any linear function $f : V \to W$ there exists a unique $m \times n$ matrix M with entries in K such that for all $v \in V : [f(v)]_{\mathscr{B}_W} = M[v]_{\mathscr{B}_V}$.*

Proof. By Proposition 2.18 we have isomorphisms $V \to K^n$ and $W \to K^m$. Via these isomorphisms we can construct a function $\tilde{f} : K^n \to K^m$ by $[v]_{\mathscr{B}_V} \mapsto [f(v)]_{\mathscr{B}_W}$. By linearity of f we find a unique $m \times n$ matrix M with entries in K such that $[f(v)]_{\mathscr{B}_W} = M[v]_{\mathscr{B}_V}$. □

This correspondence lets us connect concepts related to functions with concepts related to matrices. Let f be a linear function and let M_f be the associated matrix. The image of f corresponds to the column space $\mathrm{Col}(M_f)$ of M_f, the span of the columns of M_f. The kernel of f corresponds to the nullspace $\mathrm{Null}(M_f)$ of M_f, the space of vectors v such that $M_f v = 0$. The dimensions of these spaces are known, respectively, as the rank $\mathrm{Rank}(M_f)$ and nullity $\mathrm{Nullity}(M_f)$ of M_f. The following theorem relates the rank and nullity and is used to slightly simplify the code in Appendix A.

Theorem 2.20 (Rank-Nullity Theorem)**.** *For any $m \times n$ matrix M over a field K we have*

$$\text{Rank}(M) + \text{Nullity}(M) = n.$$

Proof. Cf. e.g. [6] p.63. □

Let g be another linear function and let M_g be its associated matrix. Then the composition $f \circ g$ of f and g corresponds to the matrix multiplication $M_f M_g$. This means that linear bijections correspond to invertible matrices, where the inverse matrix corresponds to the inverse function. We denote $\text{Mat}_n(K)$ for the set of $n \times n$ matrices over K and $\text{GL}_n(K)$ for the subset of $\text{Mat}_n(K)$ of invertible matrices.

Theorem 2.21. *The set* $\text{GL}_n(K)$ *forms a group with the operation matrix multiplication.*

Proof. Cf. e.g. [7] p.13. □

The identity element of $\text{GL}_n(K)$ is $\mathbb{1}_n$, the $n \times n$ matrix with 1's on the diagonal and 0's everywhere else.

The size of the group $\text{GL}_n(K)$ is given by the following paraphrased version of proposition 1.10.1 in [8].

Theorem 2.22. *The number of invertible $n \times n$ matrices over a field K with q elements is*

$$|\text{GL}_n(K)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Proof. An arbitrary $n \times n$ matrix is invertible if and only if its columns are independent. There are $q^n - 1$ choices for the first column; all non-zero vectors in K^n. The q multiples of the first column are all vectors dependent on it. So there are $q^n - q$ choices for the second column. The first two columns span a subspace V of K^n of dimension 2, since they are independent. The third column can be any element of K^n not in V, so there are $q^n - q^2$ choices for the third column. Continuing this reasoning we get that there are $q^n - q^{i-1}$ choices for the i-th column. □

In Theorem 3.11 there is a different kind of product of matrices: the Kronecker product. The Kronecker product is a way to combine two matrices of any size into a larger matrix containing all products between an element of the first matrix and an element of the second matrix.

Definition 2.23 (Kronecker Product)**.** *Let A be an $n \times m$ matrix with entries $\alpha_{ij} \in K$ for $1 \leq i \leq n$, $1 \leq j \leq m$ and let B be an $p \times q$ matrix. Then the* Kronecker product *of A and B is the np by mq matrix $A \otimes B$ consisting of blocks $\alpha_{ij} B$.*

This definition is better understood with an example.

Example 2.24.

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 1\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} & 2\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \\ 3\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} & 4\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 5 & 6 & 10 & 12 \\ 7 & 8 & 14 & 16 \\ 15 & 18 & 20 & 24 \\ 21 & 24 & 28 & 32 \end{bmatrix}$$

In Theorem 3.11 we also encounter an eigenspace of a matrix. Eigenspaces and eigenvalues are defined very similarly to the case over $\mathbb{R}$. The difference is that the eigenvalues exist in the scalar field K or some extension of it. We will only need the eigenspace corresponding to the eigenvalue 1, which is given by $\text{Eig}_1 = \text{Null}(M - \mathbb{1}_n)$ for an $n \times n$ matrix M.

3

Algebras

An algebra is the algebraic structure describing a product of vectors. Examples include, but are not limited to, $\mathbb{R}^3$ with the cross-product, $\mathbb{C}$ as vector space over $\mathbb{R}$ with complex multiplication and $\mathrm{Mat}_n(K)$ as vector space over a field K with matrix multiplication. The common thread is the relation between the product and the vector operations addition and scalar multiplication.

Definition 3.1 (Algebra)**.** *An* algebra *over a field K is a vector space A over K equipped with a* bilinear *product $* : A \times A \to A$, that is, for all $\alpha \in K$, $u, v, w \in A$ we have*

- $\alpha \cdot (u * v) = (\alpha \cdot u) * v = u * (\alpha \cdot v)$
- $(u + v) * w = (u * w) + (v * w)$
- $u * (v + w) = (u * v) + (u * w)$

In the literature, a symbol for multiplication is often left out. In this thesis, however, we will explicitly write $*$ to disambiguate the vector-vector product from scalar products and matrix-vector products.

Due to their underlying vector space structure, many results from linear algebra can be extended to algebras. In particular, the relationship between linear functions and matrices discussed in Chapter 2.3 gives us a relation between algebras and vectors of matrices. The group $\mathrm{GL}_n(K)$ plays a significant role in completing this correspondence. Additionally, an algebra's dimension and basis correspond to the dimension and basis of its underlying vector space.

Definition 3.2 (Algebra Isomorphism)**.** *Two algebras A and A' are said to be* isomorphic *if the vector spaces A and A' are isomorphic and an isomorphism $f : A \to A'$ respects the multiplication, that is, for any $a, b \in A$ we have $f(a *_A b) = f(a) *_{A'} f(b)$.*

We denote the isomorphism class of an algebra A as $[A]$. The set of all isomorphism classes of n-dimensional algebras over a field K is denoted as $\mathrm{Alg}_n(K)$. The size of $\mathrm{Alg}_n(K)$ is the number of non-isomorphic n-dimensional algebras over K.

Example 3.3. *Consider the vector space $\mathbb{F}_2^2$ over $\mathbb{F}_2$. Component-wise multiplication defines a bilinear map on $\mathbb{F}_2^2$. So $\mathbb{F}_2^2$ is an algebra over $\mathbb{F}_2$ with component-wise multiplication.*

Example 3.4. *Consider $\mathbb{F}_4$ as vector space over $\mathbb{F}_2$. Multiplication in $\mathbb{F}_4$ defines a bilinear map on $\mathbb{F}_4$. So $\mathbb{F}_4$ is an algebra over $\mathbb{F}_2$ with multiplication in $\mathbb{F}_4$.*

Note that $\{1, X\}$ is a basis for $\mathbb{F}_4$, so $\mathbb{F}_4 \cong \mathbb{F}_2^2$ as vector spaces. However, in $\mathbb{F}_4$ there are no non-zero elements whose product is 0, whereas in $\mathbb{F}_2^2$ we have $(0,1)^T * (1,0)^T = (0,0)$. So $\mathbb{F}_4 \ncong \mathbb{F}_2^2$ as algebras.

3.1. Vector of Matrices Representation

We have seen in Proposition 2.18 that a vector space is fully determined by its dimension and its scalar field. The examples given above show that this is clearly not the case for algebras. The bilinear product determines the rest of the structure. In his paper [9] Verhulst exploited the bilinearity of this product to represent algebras using matrices. This section is heavily based on his work.

Consider an n-dimensional algebra A over a field K with basis $\mathscr{B} = \{e_1, \ldots, e_n\}$. Let $a, b \in A$ and write $a = \sum_{i=1}^n \alpha_i e_i$ for $\alpha_i \in K$. We can now use the linearity of the multiplication to rewrite the product $a * b$.

$$\begin{aligned} a * b &= \left(\sum_{i=1}^n \alpha_i e_i \right) * b \\ &= \sum_{i=1}^n \alpha_i (e_i * b) \end{aligned}$$

We see that the product $a * b$ is determined by the products $e_i * b$ for $1 \leq i \leq n$. Using linearity in the second argument we can reduce this further to the products $e_i * e_j$ for $1 \leq i, j \leq n$. So the products of basis vectors completely determine the product of vectors. This reduces the condition on an isomorphism of algebras to $f(e_i *_A e_j) = f(e_i) *_{A'} f(e_j)$.

We can also take a slightly different approach. For $b \in A$ consider the maps $f_i : b \mapsto e_i * b$ for $1 \leq i \leq n$, then the linearity in the second argument of the product implies linearity of the functions f_i. This in turn means that there are matrices M_i associated with f_i such that $[e_i * b]_{\mathscr{B}} = [f_i(b)]_{\mathscr{B}} = M_i [b]_{\mathscr{B}}$. So the algebra A is determined by the vector of n $n \times n$ matrices $\mathscr{M} = (M_1, \cdots, M_n)^T$.

This motivates us to define the following family of algebras.

Definition 3.5. *The algebra induced by a vector $\mathscr{M}$ of n $n \times n$ matrices over a field K is the n-dimensional algebra over K with vector space structure K^n and a bilinear product given by $e_i * a = M_i a$ for every $a \in K^n$ and $i \in \{1, \cdots, n\}$. This algebra is denoted by* $\mathrm{alg}(\mathscr{M})$.

Lemma 3.6. *For every n-dimensional algebra A over a field K there is an $\mathscr{M} \in \mathrm{Mat}_n(K)^n$ such that $A \cong \mathrm{alg}(\mathscr{M})$.*

Proof. The argument above Definition 3.5 provides $\mathscr{M}$ given A. □

Example 3.7. *Consider, for example, the algebra $\mathbb{R}^3$ with the cross-product. A natural basis for $\mathbb{R}$ is $e_1 = (1,0,0)^T, e_2 = (0,1,0)^T, e_3 = (0,0,1)^T$. To describe this algebra using matrices we look at the products of e_1, e_2, e_3 with an arbitrary vector $b = (b_1, b_2, b_3)^T \in \mathbb{R}^3$.*

$$e_1 \times b = \begin{bmatrix} 0 \\ -b_3 \\ b_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = M_1 b$$

$$e_2 \times b = \begin{bmatrix} b_3 \\ 0 \\ -b_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = M_2 b$$

$$e_3 \times b = \begin{bmatrix} -b_2 \\ b_1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = M_3 b$$

We see that $\mathbb{R}^3$ *with the cross-product is induced by* $\mathscr{M} = (M_1, M_2, M_3)^T$.

Example 3.8. *Consider the matrices*

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{F}_2)$$

They define a bilinear product on the vector space $\mathbb{F}_2^2$ *by associating the first matrix with multiplication on the left by* $(1,0)^T$ *and the second matrix with multiplication on the left by* $(0,1)^T$. *Let* $(a,b)^T, (c,d)^T \in \mathbb{F}_2^2$. *Then their product is given by*

$$\begin{aligned} \begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} c \\ d \end{bmatrix} &= a \cdot \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} * \begin{bmatrix} c \\ d \end{bmatrix} \right) + b \cdot \left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} * \begin{bmatrix} c \\ d \end{bmatrix} \right) \\ &= a \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} + b \cdot \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} c \\ d \end{bmatrix} \\ &= \begin{bmatrix} a \cdot c \\ a \cdot d \end{bmatrix} + \begin{bmatrix} b \cdot d \\ b \cdot (c+d) \end{bmatrix} \\ &= \begin{bmatrix} a \cdot c + b \cdot d \\ a \cdot d + b \cdot c + b\dot{d} \end{bmatrix} \end{aligned}$$

We see how two matrices induce a 2-dimensional algebra over $\mathbb{F}_2$.

Note that there are different vectors of matrices that correspond to isomorphic algebras. Multiplying all matrices with the same non-zero element will result in an isomorphic algebra. In other words, the map

$$\begin{aligned} [\mathrm{alg}] : \mathrm{Mat}_n(K)^n &\to \mathrm{Alg}_n(K) \\ \mathscr{M} &\mapsto [\mathrm{alg}(\mathscr{M})] \end{aligned}$$

is surjective (Lemma 3.6), but not injective.

Lemma 3.9. *Given two vectors of matrices* $\mathscr{M} = (M_1, \ldots, M_n), \mathscr{N} = (N_1, \ldots, N_n) \in \mathrm{Mat}_n(K)^n$. *The algebras* $\mathrm{alg}(\mathscr{M})$ *and* $\mathrm{alg}(\mathscr{N})$ *are isomorphic if and only if*

$$\exists G \in \mathrm{GL}_n(K) : M_i = G^{-1}(\sum_{k=1}^{n} G_{ki} N_k) G.$$

Proof. Suppose that $\mathrm{alg}(\mathscr{M})$ and $\mathrm{alg}(\mathscr{N})$ are isomorphic. Then there exists an isomorphism $f : \mathrm{alg}(\mathscr{M}) \to \mathrm{alg}(\mathscr{N})$. So f is a linear bijection such that for a basis $\{e_1, \ldots, e_n\}$ for A_M we have $f(e_i * e_j) = f(e_i) * f(e_j)$ for $1 \leq i, j \leq n$. So there is a matrix $G \in \mathrm{GL}_n(K)$ associated with f such that $G(e_i * e_j) = Ge_i * Ge_j$. Using the vectors of matrices we can rewrite

$$\begin{aligned} G(e_i * e_j) &= GM_i e_j \\ Ge_i * Ge_j &= \sum_{k=1}^{n} G_{ki} e_k * Ge_j \\ &= (\sum_{k=1}^{n} G_{ki} N_k) Ge_j \end{aligned}$$

Multiplying both sides on the left with G^{-1} we find $M_i e_j = G^{-1}(\sum_{k=1}^{n} G_{ki} N_k G) e_j$. Since the matrices act the same on all basis vectors, we have the desired result.

Conversely, suppose there exists a $G \in \mathrm{GL}_n(K)$ such that $M_i = G^{-1}(\sum_{k=1}^{n} G_{ki} N_k) G$. Then G induces a linear bijection $f : \mathrm{alg}(\mathscr{M}) \to \mathrm{alg}(\mathscr{N})$. It suffices to show that $f(e_i * e_j) = f(e_i) * f(e_j)$. Using the hypothesis ($Hyp.$) we find

$$\begin{aligned} f(e_i) * f(e_j) = Ge_i * Ge_j &= (\sum_{k=1}^{n} G_{ki} N_k) Ge_j \\ &= GG^{-1}(\sum_{k=1}^{n} G_{ki} N_k) Ge_j \overset{Hyp.}{=} GM_i e_j = f(e_i * e_j) \end{aligned}$$

□

Let $\phi : \mathrm{Mat}_n(K)^n \times \mathrm{GL}_n(K) \to \mathrm{Mat}_n(K)^n$ be given by

$$\phi\left(\begin{bmatrix} M_1 \\ \vdots \\ M_n \end{bmatrix}, G\right) = \begin{bmatrix} G^{-1}(\sum_{k=1}^{n} G_{k1} N_k) G \\ \vdots \\ G^{-1}(\sum_{k=1}^{n} G_{kn} N_k) G \end{bmatrix}$$

As we have seen in Section 2.3, the invertible matrices $\mathrm{GL}_n(K)$ form a group with operation matrix multiplication.

Lemma 3.10. *The map ϕ defines a $\mathrm{GL}_n(k)$-action on $\mathrm{Mat}_n(K)$.*

Proof. It is easy to see that $\phi(\mathscr{M}, \mathbb{1}_n) = \mathscr{M}$ for any $\mathscr{M} \in \mathrm{Mat}_n(K)^n$. Let $\mathscr{M} = (M_1, \ldots, M_n)^T \in \mathrm{Mat}_n(K)^n$ and $G, G' \in \mathrm{GL}_n(K)$.

$$\begin{aligned} \phi(\phi(\mathscr{M}, G), G') &= \phi\left(\begin{bmatrix} G^{-1}\sum_{k=1}^{n} G_{k1} M_k G \\ \vdots \\ G^{-1}\sum_{k=1}^{n} G_{kn} M_k G \end{bmatrix}, G'\right) = \begin{bmatrix} G'^{-1}\sum_{l=1}^{n} G'_{l1}(G^{-1}\sum_{k=1}^{n} G_{kl} M_k G) G' \\ \vdots \\ G'^{-1}\sum_{l=1}^{n} G'_{ln}(G^{-1}\sum_{k=1}^{n} G_{kl} M_k G) G' \end{bmatrix} \\ &= \begin{bmatrix} GG'^{-1}\sum_{k=1}^{n} (GG')_{k1} M_k GG' \\ \vdots \\ GG'^{-1}\sum_{k=1}^{n} (GG')_{kn} M_k GG' \end{bmatrix} = \phi(\mathscr{M}, GG') \end{aligned}$$

□

By Lemma 3.9 two vectors of matrices are in the same orbit if and only if the algebras they induce are isomorphic. This implies that the following map is injective.

$$\overline{\text{alg}} : \text{Mat}_n(K)^n / \text{GL}_n(K) \to \text{Alg}_n(K), (\text{GL}_n(K))(\mathcal{M}) \mapsto [\text{alg}(\mathcal{M})]$$

Since the map [alg] is surjective, this map is also surjective. So the map $\overline{\text{alg}}$ is a bijection between the orbits of $\text{Mat}_n(K)^n$ under ϕ and the set of non-isomorphic algebras $\text{Alg}_n(K)$. This means that there are as many elements in $\text{Alg}_n(K)$ as there are orbits of $\text{Mat}_n(K)$ under ϕ. These orbits can be counted using Burnside's lemma, which is exactly what Verhulst [9] did in 2020 to obtain the following result.

Theorem 3.11. *The number of non-isomorphic n-dimensional algebras over $K = \mathbb{F}_q$ is*

$$|\text{Alg}_n(K)| = \frac{1}{|\text{GL}_n(K)|} \sum_{M \in \text{GL}_n(K)} q^{\dim \text{Eig}_1(M^T \otimes M^T \otimes M^{-1})}.$$

4

Data and Analysis

Using Theorem 3.11 we can calculate the number of n-dimensional algebras over a field with q elements. In this chapter we discuss my implementation in python (see Appendix A) of the formula in Theorem 3.11 and the results that it provided.

4.1. Some Notes on the Code

The main function is $AlgebraCount(n,q)$. It starts by initiating the finite field K with q elements using the $galois$ package [3]. This package is an implementation of the finite fields into python and is designed to be compatible with numpy. Next the function $\mathrm{GL}(n,q)$ is called to make a list of all invertible $n \times n$ matrices over K. This function checks a list of all $n \times n$ matrices over the field K for invertible matrices and returns them in a list. The function $\mathrm{Mat}(n,q)$ generates this list of all matrices. This is done using a bijection from the numbers 0 through $q^{n^2}-1$ written in base q.

Example 4.1. *Suppose for example that we want to generate a list of all* 2×2 *matrices over* $\mathbb{F}_3$. *List these matrices by varying one component at a time. The start of such a list would look like*

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

This way of listing is very reminiscent of listing integers in base 3. If we consider the first entry of a matrix to be the number of units, the second to be the number of threes, the third to be the number of nines and the fourth to be the number of 27's. Then the list of matrices corresponds to the list of base 3 numbers

$$0000,0001,0002,0010,0011,0012,0020,0021,\cdots$$

which corresponds with the list of base 10 numbers

$$0,1,2,3,4,5,6,7,\cdots$$

Since there are 3^{2^2} *different* 2 *by* 2 *matrices over* $\mathbb{F}_3$, *we can easily use this to list all matrices.*

The functions $base(x,q)$ and $ListtoMatrix(lst,n)$ each implement one of the steps in the conversion from the numbers 0 through $q^{n^2}-1$ to the list of all matrices. Note that the

galois package has an integer representation for elements of a finite field $\mathbb{F}_q$ even if q is not prime. So even though 8 is not actually an element of the field $\mathbb{F}_9$, it still represents one of the elements of $\mathbb{F}_9$, and when viewed as an element of $\mathbb{F}_9$ it will act like the element it is supposed to represent.

Having generated a list $GLnK$ of all $n \times n$ invertible matrices over K, $AlgebraCount$ iterates through $GLnK$ to calculate the contribution of each matrix and add them as in Theorem 3.11. First, it calculates the Kronecker product of the matrix's transpose with itself and with its inverse. This results in the $n^3 \times n^3$ matrix TTI.

The variable $dimEig1$ represents the dimension of the eigenspace corresponding to the eigenvalue 1 of TTI. By definition this eigenspace is given by $\text{Null}(TTI - 1 \cdot \mathbb{1}_{n^3})$. Seeing as $dimEig1$ is the dimension of the nullspace of $TTI - \mathbb{1}_{n^3}$, we can use the Rank-Nullity Theorem 2.20 to calculate it. So

$$dimEig1 = n^3 - \text{Rank}(TTI - \mathbb{1}_{n^3}).$$

Note that numpy by default makes $dimEig1$ a 32-bit integer. This is not a problem for $dimEig1$ as it stays relatively small. However, this also makes $q^{dimEig1}$ a 32-bit integer, causing overflow errors to occur. To circumvent this, $dimEig1$ is converted to a standard python integer first to allow for arbitrary size.

Lastly, the contribution $q^{dimEig1}$ of each matrix is added to the total and the total divided by the length of $GLnK$ is returned.

4.2. Results

In Table 4.1 we see the output of $AlgebraCount(n, q)$ for certain n and q.

Table 4.1: Output of $AlgebraCount(n, q)$

$q \setminus n$	1	2	3	4
2	2	52	801 168	915 017 470 109 856
3	2	162	678 999 898	
4	2	402	99 286 246 390	
5	2	877	5 007 115 325 062	
7	2	2 975	1 945 066 184 799 352	
8	2	4 894		
9	2	7 656		
11	2	16 507		

For $n = 1$ and any prime power q, there are 2 non-isomorphic algebras. The only non-isomorphic 1-dimensional algebras over $\mathbb{F}_q$ are $\mathbb{F}_q^1$ with field multiplication and $\mathbb{F}_q^1$ with all products equal to 0. This result can also be independently derived.

Theorem 4.2. *For any prime power q all 1-dimensional algebras over $\mathbb{F}_q$ are either isomorphic to $\mathbb{F}_q$ with field multiplication or to $\mathbb{F}_q$ with every vector product equal to 0.*

Proof. Without loss of generality the vector space is $\mathbb{F}_q^1$. Let $\mathbb{F}_q^1$ be an algebra over $\mathbb{F}_q$ with the product given by $1 * 1 = \alpha \in \mathbb{F}_q^1$. Suppose $\alpha = 0$. Then for any $u, v \in \mathbb{F}_q^1$ we have $u * v = uv(1 * 1) = uv0 = 0$. So $\mathbb{F}_q^1$ is the algebra where every product is equal to 0. Now suppose

$\alpha \neq 0$. Then $\alpha^{-1} * \alpha^{-1} = \alpha^{-1}\alpha^{-1}(1*1) = \alpha^{-1}\alpha^{-1}\alpha = \alpha^{-1}$. Let $\mathbb{F}'_q$ be the algebra over $\mathbb{F}_q$ with field multiplication and let $f : \mathbb{F}'_q \to \mathbb{F}^1_q$ be the linear bijection given by $f(1) = \alpha^{-1}$. Then we have $f(1*1) = f(1) = \alpha^{-1} = \alpha^{-1} * \alpha^{-1} = f(1) * f(1)$. So f is an isomorphism and $\mathbb{F}^1_q$ is isomorphic to the algebra with field multiplication. □

For $n = 2$ and any $q \leq 41$, the results have been verified with the polynomial formulas by Petersson and Scherer [5]. My expectation is that the code will keep matching the polynomial formulas for $q > 41$, but due to limits in computation time I have not yet been able to verify this.

For $n = 3$ and $n = 4$, the results in Table 4.1 are, to my knowledge, new. Currently the limiting factor to getting more results is computation time. My laptop took about 3 days to calculate the number for $n = 3$, $q = 7$ and about 4 minutes to calculate the number for $n = 4$, $q = 2$. I have tried calculating the number for $n = 4$, $q = 3$, but killed the program after about 5 days. Similarly, for $n = 5$, $q = 2$ I killed the program after about 5 days.

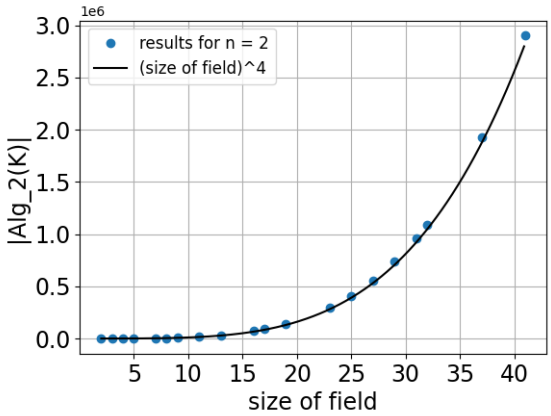

Figure 4.1: The number of non-isomorphic 2-dimensional algebras over a field with q elements changes approximately like q^4.

Figure 4.1 was made using the results for $n = 2$, but might as well have been made using the polynomial formulas by Petersson and Scherer [5]. Seeing as these polynomials in q all have degree 4, it might seem obvious that q^4 is a close approximation of the number of non-isomorphic 2-dimensional algebras. However, when seeing this with Theorem 3.11 in mind one might notice a possible generalisation.

Consider the contribution of the identity matrix to the number of non-isomorphic algebras. The transpose and the inverse of the identity matrix are equal to the identity matrix and the Kronecker product of the identity matrix with itself is a bigger identity matrix. So for $n = 2$ we have

$$\mathbb{1}_2^T \otimes \mathbb{1}_2^T \otimes \mathbb{1}_2^{-1} = \mathbb{1}_2 \otimes \mathbb{1}_2 \otimes \mathbb{1}_2 = \mathbb{1}_8.$$

Note that all eigenvalues of the identity matrix are equal to 1, since $\mathbb{1}_8 v = 1v$ for all v. So the dimension of the corresponding eigenspace is equal to the size of the identity matrix. So in the case that $n = 2$ this dimension is 8 and the identity matrix contributes q^8 to the sum. By Theorem 2.22 we have that the number of invertible 2×2 matrices over a field K with q elements is

$$|\mathrm{GL}_2(K)| = (q^2 - 1)(q^2 - q) = q^4 - q^3 - q^2 + q.$$

Putting these together we find that the total contribution of the identity matrix is

$$\frac{q^8}{q^4 - q^3 - q^2 + q},$$

which approaches q^4 as q goes to infinity. This suggests that the identity matrix is the most important matrix, which makes sense considering it is the only matrix all of whose eigenvalues are equal to 1. Using this strategy we find the following lower bound.

Theorem 4.3. *The number of non-isomorphic n-dimensional algebras over $K = \mathbb{F}_q$ is bound from below by $q^{n^3-n^2}$.*

Proof. Considering just the identity matrix in Theorem 3.11 we get

$$\begin{aligned} |\mathrm{Alg}_n(K)| &\geq \frac{1}{|\mathrm{GL}_n(K)|} q^{\dim \mathrm{Eig}_1(\mathbb{1}_n^T \otimes \mathbb{1}_n^T \otimes \mathbb{1}_n^{-1})} \\ &= \frac{1}{|\mathrm{GL}_n(K)|} q^{\dim \mathrm{Eig}_1(\mathbb{1}_{n^3})} \\ &= \frac{1}{|\mathrm{GL}_n(K)|} q^{n^3}. \end{aligned}$$

Rounding all factors up to q^n in Theorem 2.22 we get

$$\begin{aligned} |\mathrm{GL}_n(K)| &= (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \\ &\leq (q^n)(q^n)(q^n) \cdots (q^n) \qquad (n \text{ copies}) \\ &= (q^n)^n = q^{n^2}. \end{aligned}$$

Putting these together we find $|\mathrm{Alg}_n(K)| \geq q^{n^3-n^2}$. □

This aggressive bound looks clean, but is not very tight. Omitting the last step of bounding $|\mathrm{GL}_n(K)|$ and thus calculating the contribution of the identity matrix, makes for a better bound.

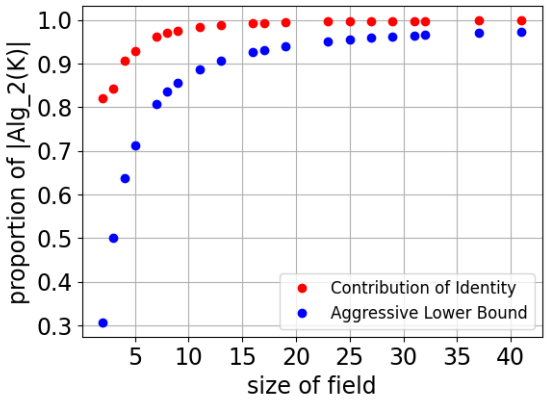

Figure 4.2: For both bounds on the number of non-isomorphic 2-dimensional algebras over a field, the proportion they account for is plotted against the size of the field.

In Figure 4.2 we see that the aggressive lower bound is not very tight for small fields. The first time it accounts for 90% of the number of non-isomorphic 2-dimensional algebras is for $q = 13$. The bound does seem to get better for bigger fields, but the absolute difference with the actual number of non-isomorphic algebras still increases, since the number of non-isomorphic algebras increases greatly.

With slightly more computations we can calculate the contribution of the identity matrix and have a bound which accounts for 99% of the total number of non-isomorphic 2-dimensional algebras for $q = 13$. The importance of the identity matrix becomes even more apparent in Figure 4.3. Even for the smallest fields, the contribution of the identity matrix accounts for 99% of the number of non-isomorphic 3-dimensional algebras.

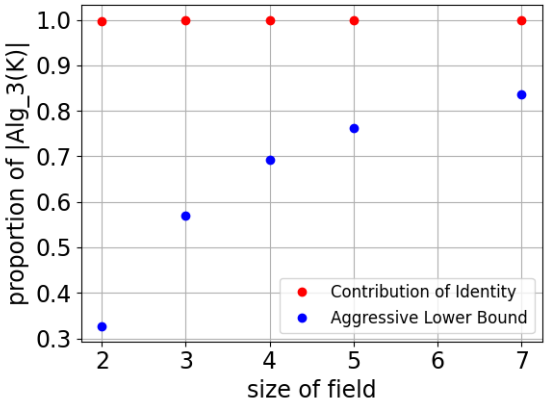

Figure 4.3: For both bounds on the number of non-isomorphic 3-dimensional algebras over a field, the proportion they account for is plotted against the size of the field.

4.3. Conclusion and Outlook

The results in Table 4.1 seem to have reached the limits of Verhulst's formula (Theorem 3.11). With more computation time or a more powerful computer it might be possible to squeeze out results for $n = 3$, $q = 8$ and $n = 4$, $q = 3$ and perhaps $n = 5$, $q = 2$. However, a more efficient formula is necessary to truly get general results. In his paper Verhulst [9] uses the Jordan normal form to work out the case $n = 2$, $q = 2$. I suspect this approach could lead to a better formula for $n = 3$ and general q. In the mean time, one can use the contribution of the identity matrix, as it has proven to be a fairly good approximation.

A

Code

```
from math import *
import time
import numpy as np
import galois                                   #implements the finite fields


# the final formula [N.D. Verhulst, 2020]
def AlgebraCount(n,q):
    K = galois.GF(q)                            #the field to work over
    GLnK = GL(n,q)                              #list of invertible matrices
    total = 0
    for M in GLnK:
        M = M.view(K)
        TTI = np.kron(np.kron(np.transpose(M), np.transpose(M)), np.linalg.inv(M))
                    #transpose kronecker transpose kronecker inverse
        dimEig1 = n**3 - np.linalg.matrix_rank(TTI - np.identity(n**3,int).view(K))
                    #dimension of the eigenspace with eigenvalue 1
        dimEig1 = int(dimEig1)                  #int to prevent overflow errors
        total += q**dimEig1                     #sum the contribution of each matrix
    return total/len(GLnK)

# gives a list of all nxn matrices over Fq
def Mat(n,q):
    O = np.zeros((n,n),int)                     #matrix of zeroes
    MatnK = np.array([O]*(q**(n**2)))           #initiating the list of matrices
    for m in range(q**(n**2)):
        basemq = base(m,q)                      #m base q represented by a list
        MatnK[m] = ListToMatrix(basemq,n)       #basemq becomes matrix
    return MatnK

# gives a list of all invertible nxn matrices over Fq
def GL(n,q):
```

```
    K = galois.GF(q)                          #the field
    O = np.zeros((n,n),int)                   #matrix of zeroes
    length = NumberGL(n,q)                    #the number of invertible matrices
    GLnK = np.array([O]*length)               #initiate list
    i = 0
    Matnq = Mat(n,q)
    for M in Matnq:
        M = M.view(K)
        if np.linalg.matrix_rank(M) == n:     #matrix is invertible
            GLnK[i] = M                       #  iff of full rank
            i += 1
    return GLnK

# |GL_n(K)| function [R.P. Stanley, 2012]
def NumberGL(n,q):
    res = 1
    for i in range(n):
        res *= q**n - q**i
    return res

# writes x in base q in a list starting with units
# e.g. base(24,3) = [0,2,2], because 24 = 0*(3**0) + 2*(3**1) + 2*(3**2)
#  and base(195,16) = [3,12], because 195 = 3*(16**0) + 12*(16**1)
def base(x,q):
    L = 0
    while q**(L+1) <= x:                      #L is log_q(x) rounded down
        L += 1
    res = np.zeros(L+1,int)
    for i in range(L+1):
        res[-i-1] = int(x/q**(L-i))
        x -= res[-i-1]*q**(L-i)
    return res

# takes a list and makes it an nxn square matrix with zeroes to fill
def ListToMatrix(lst,n):
    M = np.zeros((n,n),int)
    for i in range(len(lst)):
        j = base(i,n)
        if len(j) == 1:
            j = np.append(j,0)
        j = tuple([j[1],j[0]])
        M[j] = lst[i]
    return M
```

Bibliography

[1] I.T. Adamson. *Introduction to Field Theory*. Oliver & Boyd, 1964.

[2] S.C. Althoen and K.D. Hansen. Two-dimensional real algebras with zero divisors. *Acta Scientiarum Mathematicarum*, 56, 01 1992.

[3] M. Hostetter. *Galois: A performant NumPy extension for Galois fields*, 11 2020. URL `https://github.com/mhostetter/galois`.

[4] H.P. Petersson. The classification of two-dimensional nonassociative algebras. *Results in Mathematics*, 37, 03 2000. doi: 10.1007/BF03322518.

[5] H.P. Petersson and M. Scherer. The number of nonisomorphic two-dimensional algebras over a finite field. *Results in Mathematics*, 45:137–152, 2004. ISSN 1420-9012. doi: 10.1007/BF03323003.

[6] S. Roman. *Advanced Linear Algebra*. Graduate Texts in Mathematics. Springer, 3 edition, 2013. ISBN 978-1-4757-2178-2. doi: https://doi.org/10.1007/978-1-4757-2178-2.

[7] J.J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer, 4 edition, 2012. ISBN 978-1-4612-4176-8. doi: https://doi.org/10.1007/978-1-4612-4176-8.

[8] R.P. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, 2 edition, 2012. ISBN 9781139058520.

[9] N.D. Verhulst. Counting finite-dimensional algebras over finite field. *Results in Mathematics*, 75, 2020. ISSN 1420-9012. doi: 10.1007/s00025-020-01281-6.