THE TENSOR RANK OF SEMIFIELDS OF ORDER 16 AND 81

MICHEL LAVRAUW AND JOHN SHEEKEY

Abstract. We determine the tensor rank of all semifields of order 16 over $\mathbb{F}_2$ and of all semifields of order 81 over $\mathbb{F}_3$. Our results imply that some semifields of order 81 have lower multiplicative complexity than the finite field $\mathbb{F}_{81}$ over $\mathbb{F}_3$. We prove new results on the correspondence between linear codes and tensor rank, including a generalisation of a theorem of Brockett and Dobkin to arbitrary tensors, which makes the problem computationally feasible.

1. Introduction

Tensors are fundamental mathematical objects which arise in a wide variety of pure and applied problems. The tensor rank is of great importance for many of these problems. Except for the two-fold tensors, which correspond to matrices, and in which case the theory of rank and equivalence (under the natural action of associated general linear groups) is straightforward and well understood, the testing of equivalence and the calculation of the tensor rank are both theoretically and computationally difficult for $k$-fold tensors for $k \geq 3$. See for example [5], [10], and [11], where it was proved that tensor rank is NP-complete for any finite field and NP-hard for the rational numbers. Recent computational results for tensors over small fields have been carried out in for example [3], [22].

The multiplicative structure of a (not necessarily associative) $n$-dimensional algebra over a field $\mathbb{F}$ can be represented by a tensor in $\mathbb{F}^n \otimes \mathbb{F}^n \otimes \mathbb{F}^n$, and tensor equivalence corresponds to algebra isotopism. The tensor rank (over some field containing $\mathbb{F}$ and contained in the centre of the algebra) then gives a measure of the complexity of multiplication in the algebra, and is invariant under equivalence, see e.g. Burgisser et al. [5].

In this paper we consider the problem of computing the tensor rank of finite semifields, that is, division algebras over a finite field where multiplication is not necessarily associative. Finite semifields have been studied since Dickson constructed the first nontrivial examples in the early 1900’s [8]. Semifields over the real numbers date back even further, to Graves’ construction of the octonions. Tensors (and the related concept of hypercubes) have been used to study semifields by Knuth [12], Liebler [19], and the first author of this paper [13], in which the tensor rank of a semifield was introduced as an isotopism invariant. Until now, due to the hardness of the problem, there had been no known theoretical or computational proof for the existence of semifields of the same order with different tensor rank. For example, it was shown in [14] that all semifields of order $3^4$ have the same tensor rank.

In this paper we determine the tensor rank of all semifields of order $3^4$, and obtain the first proof for the existence of semifields of the same order with different tensor rank. This establishes the tensor rank as a non-trivial invariant for the isomorphism classes of finite semifields. Most notably, the tensor rank of most of the semifields of order $3^4$ is one less than the tensor rank of the finite field of order $3^4$. By virtue of the relationship between the complexity of multiplication and the tensor rank, this gives these semifields a significant computational advantage for applications. The following theorem is the main result of this paper.

Theorem 1. The field and generalised twisted field of order $3^4$ each have tensor rank nine over $\mathbb{F}_3$. All other semifields of order $3^4$ have tensor rank eight over $\mathbb{F}_3$.

The proof consists of both a theoretical and a computational component.
The paper is organised as follows. In Section 2.1 we introduce some of the background on tensors, and their contractions spaces. In Section 2.2 we introduce the necessary theory on semifields and their relation with nonsingular tensors. We include a first result on the automorphism group of the spread set of the finite field, which will be used in proving the main result. In the next section, Section 2.3 we use the link between tensor rank and the minimum distance of a linear code. This section includes a slight generalisation of the result by Brockitt and Dobkin from [4], which will assist us in speeding up the algorithms and make them computationally feasible. In the final subsection of Section 2 we give an overview of the relevant known results on tensor ranks.

Based on these theoretical results, in Section 3 we describe the algorithms which were used to determine the tensor rank of all semifields of order $2^4$ and $3^4$.

In Section 4 it is shown how the theoretical results allow for the computation of the tensor rank of all semifields of order $2^4$. This leads to Theorem 3 which confirms that every semifield of order $2^4$ has tensor rank 9 over $\mathbb{F}_2$.

Finally, in Section 5, the theoretical results are applied to the computation of the tensor rank over $\mathbb{F}_3$ of semifields of order $3^4$, leading to the main result of this paper. Computationally this is by far the most significant part of our results. We provide the necessary computational data which should allow the reader to verify our results.

2. Definitions and Preliminary Results

2.1. Tensors and Contraction Spaces. Here we recall the necessary definitions regarding tensors.

Let $V = \bigotimes_{i=1}^t V_i$ denote the tensor product of the finite-dimensional vector spaces $V_i$, $i \in \{1, \ldots, t\}$. The elements $v = v_1 \otimes \cdots \otimes v_t$ are called fundamental tensors, or pure tensors. We say that elements of $V$ are tensors of order $t$.

Every tensor $T \in V$ can be written as a sum of pure tensors. We refer to an expression

$$T = \sum_{j=1}^R v_{j_1} \otimes \cdots \otimes v_{j_t}$$

as a decomposition of $T$ into the sum of $R$ pure tensors.

**Definition 1.** The tensor rank of $T$ is the minimum nonnegative integer $R$ such that there exists a decomposition of $T$ into $R$ pure tensors. It is denoted by $\text{trk}(T)$.

The pure tensors are then by definition the tensors of rank one.

The group $G = \prod_i \text{GL}(V_i)$ acts on pure tensors in the natural way:

$$(g_1, \ldots, g_t) : v_1 \otimes \cdots \otimes v_t \mapsto g_1(v_1) \otimes \cdots \otimes g_t(v_t).$$

This can be extended to define an invertible linear transformation on $V$, and so we have that $G \leq \text{GL}(V)$.

The group $G$ setwise stabilises the set of pure tensors in $\text{GL}(V)$.

Two tensors are $G$-equivalent (or just equivalent if $G$ is clear from the context) if they are in the same $G$-orbit of $V$. Clearly, $G$-equivalent tensors have the same tensor rank.

If $v_i$ is an element of the dual space $V_i^\vee$ of $V_i$, we define the contraction of $v = v_1 \otimes \cdots \otimes v_t$ by $v_i$ as

$$v_i(v) := v_i(v_i(v_1 \otimes \cdots \otimes v_{i-1} \otimes v_{i+1} \otimes \cdots \otimes v_t)) \in \bigotimes_{j \neq i} V_j.$$

This can be extended linearly to define $v_i(T)$ for any tensor $T \in V$. Given a subspace $U$ of $V$ we can also naturally define $v_i(U)$, which is a subspace of $\bigotimes_{j \neq i} V_j$. An important concept is that of the so-called contraction space of a tensor, defined as follows.
In particular, if two algebras over $F$ are isotopic, then their tensor ranks over $F$ are equal.

We state the following lemma without proof; see for example [13], where the result is proved for a special case, but the proof is identical.

**Lemma 2.** The tensor rank of $T \in V$ is equal to the minimum number of pure tensors in $\otimes_{j \neq i} V_j$ whose span contains $C_i(T)$.

The following is well known, see e.g. [13] for a proof.

**Lemma 1.** The tensor rank of $T \in V$ is equal to the minimum number of pure tensors in $\otimes_{j \neq i} V_j$ whose span contains $C_i(T)$.

The group $G_i = \prod_{j \neq i} \text{GL}(V_j)$ acts on $\otimes_{j \neq i} V_j$. We define the automorphism group of $C_i(T)$ to be the setwise stabiliser of $C_i(T)$ in $G_i$.

We will mainly focus on the case $V_1 \simeq V_2 \simeq V_3 \simeq F_q^n$, and on the first contraction space $C_1(T)$. Denoting by $M_n(F_q)$ the $F_q$-vector space of $n \times n$ matrices with entries from $F_q$, we may identify $v_i^\vee(T)$ with an element of $M_n(F_q)$, and $C_1(T)$ with a subspace of $M_n(F_q)$ of dimension at most $n$.

### 2.2. Tensors, Algebras, and Semifields

Let $V = F_q^n$ be an $n$-dimensional vector space over $F_q$. Let us recall the following correspondence between 3-fold tensors and algebras. We follow the notation and terminology from [13, Section 4.2] to which we refer for further details on this correspondence.

Given a tensor $T = \sum_i a_i^\vee \otimes b_i^\vee \otimes z_i$ in $V^\vee \otimes V^\vee \otimes V$, it is well known that we can define an algebra $A_T = (V, \circ_T)$ with (not necessarily associative) $F_q$-bilinear multiplication $\circ_T : V \times V \rightarrow V : (x, y) \mapsto x \circ_T y$ by

$$x \circ_T y := \sum_i a_i^\vee(x)b_i^\vee(y)z_i.$$  

Conversely, an algebra $A = (V, \circ)$ with $F_q$-bilinear multiplication $\circ$ defines a homomorphism from $V \otimes V$ to $V$, mapping $x \otimes y$ to $x \circ y$. As $\text{Hom}(V \otimes V, V)$ is isomorphic to $V^\vee \otimes V^\vee \otimes V$, from $\circ$ we can define a tensor $T_A$. With appropriate choices of isomorphisms, we have that $T_A \simeq T$, and $T_{A_T} = A$.

As $(F_q^n)^\vee$ is isomorphic to $F_q^n$ as a vector space, we may fix an isomorphism and abuse notation a little by identifying $T_A$ with an element of $F_q^n \otimes F_q^n \otimes F_q^n$.

**Definition 3.** The tensor rank of an algebra $A$ over $F_q$ is defined as the tensor rank of the tensor $T_A$.

Note that an algebra with centre $F_q$ can also be regarded as an algebra over any subfield of $F_q$. For example the finite field $F_{q^2}$ is a one-dimensional algebra over itself, in which case it has tensor rank one, but also as a two-dimensional algebra over $F_q$, in which case it has tensor rank three (see [17]). For the rest of this paper we will fix a field $F_q$ and consider all algebras as $n$-dimensional algebras over $F_q$. We will refer to its tensor rank as its tensor rank over $F_q$, even if its centre is in fact strictly larger than $F_q$.

**Definition 4.** Two algebras $A = (V, \circ)$ and $B = (V, \ast)$ with centre containing $F_q$ are said to be isotopic if there exist invertible $F_q$-linear maps $f, g, h \in \text{GL}(V)$ such that

$$f(x \circ y) = g(x) \ast h(y)$$

for all $x, y \in V$. The triple $(f, g, h)$ is called an isotopism.

We state the following lemma without proof; see for example [13], where the result is proved for a special case, but the proof is identical.

**Lemma 2.** Two algebras $A$ and $B$ over $F_q$ are isotopic if and only if the tensors $T_A$ and $T_B$ are equivalent. In particular, if two algebras over $F_q$ are isotopic, then their tensor ranks over $F_q$ are equal.

In this paper we are particularly interested in algebras known as semifields.

**Definition 5.** A finite presemifield over $F_q$ is a vector space $F_q^n$ together with an $F_q$-bilinear multiplication $\circ : F_q^n \times F_q^n \rightarrow F_q^n : (x, y) \mapsto x \circ y$ such that $x \circ y = 0$ if and only if $x = 0$ or $y = 0$. If this multiplication possesses an identity element, then we refer to it as a finite semifield.
It is straightforward to check that each of these elements has rank one, since the image of \( \text{Tr}(\cdot) \) we will refer to as \( C \) has rank as an 
There are many other known constructions; see [15] for an overview. From a presemifield there exists here. If we consider the extension field \( F \) effective. We note that the definition for infinite semifields is more nuanced; we will limit ourselves to the finite 
In other words, a finite semifield is a finite division algebra in which multiplication is not necessarily associative. We note that the definition for infinite semifields is more nuanced; we will limit ourselves to the finite case here. If we consider the extension field \( F \) as outlined above. The tensors corresponding to presemifields are precisely the nonsingular tensors [13]. All presemifields are isotopic to a semifield, using Kaplansky’s trick; see [15]. For theoretical 
Definition 6. A spread set associated to a presemifield \( S \) is the set of endomorphisms of \( F_q^n \) defined by left-multiplication, namely
\[
C_S := \{ L_x : y \mapsto x \circ y \}.
\]
It is not difficult to see that \( C_S \) can be identified with \( C_1(T_S) \). Furthermore every nonzero element of \( C_S \) is invertible. Thus presemifields can equally be studied as \( n \)-dimensional subspaces of \( M_n(F_q) \). The following result can be found in [13], and is a special case of Lemma 1 above.
Lemma 3. The tensor rank of a presemifield \( S \) of dimension \( n \) over \( F_q \) is equal to the minimum number of rank one matrices in \( M_n(F_q) \) whose span contains a spread set associated to \( S \).

As mentioned above, isotopic presemifields have the same tensor rank. We note here that there is a natural \( S_3 \)-action on tensors in \( F^n \otimes F^n \otimes F^n \) which preserves nonsingularity, which produces a set of up to six isotopism classes of presemifields associated to a single presemifield, known as the Knuth orbit [12]. Again we refer to [13] for the following.
Lemma 4. The tensor rank of a presemifield is a Knuth orbit invariant.

Thus when calculating the tensor rank of a presemifield, we may choose any representative for any of the isotopism classes of its Knuth orbit. 

We end this section, with the following lemma which will assist with speeding up the calculation of the tensor rank of \( F_q^n \) over \( F_q \).

Lemma 5. The automorphism group of a spread set of the field \( F_q^n \) in \( M_n(F_q) \) acts transitively on rank one matrices.

Proof. It is well-known that the ring of \( n \times n \)-matrix over \( F_q \) is isomorphic to the ring of linearized polynomials of degree at most \( q^{n-1} \) (that is, polynomials in \( F_q[x] \) of the form \( f(x) = \sum_{i=0}^{n-1} f_i x^q^i \) with operations polynomial addition and composition modulo \( x^{q^n} - x \). The rank of a linearized polynomial is defined as its rank as an \( F_q \)-linear map from \( F_q^n \) to itself.

The image of a spread set of the field \( F_q^n \) corresponds to the set \( \{ ax : a \in F_q^n \} \), which by abuse of notation we will refer to as \( C_{\phi_n} \). It is straightforward to verify that the automorphism group of \( C_{\phi_n} \) contains the set \( \{ (ax, bx) : a, b \in F_q^n \} \). In fact the full automorphism group is the set \( \{ (ax^q^i, bx^q^{n-1}) : a, b \in F_q^n \} \), but we do not require this fact.

It is also well-known that the set of rank one matrices corresponds to the set \( \{ a\text{Tr}(bx) : a, b \in F_q^n \} \), where \( \text{Tr}(x) = \sum_{i=0}^{n-1} x^q^i \) is the linearized polynomial corresponding to the relative trace map from \( F_q^n \) to \( F_q \). It is straightforward to check that each of these elements has rank one, since the image of \( a\text{Tr}(bx) \) is the
one-dimensional $\mathbb{F}_q$-subspace defined by $a$. A simple counting argument verifies that all rank one elements are of this form.

Now consider the element $\text{Tr}(x)$ of rank one. Its image under the element $(ax, bx)$ is $(ax) \circ \text{Tr}(x) \circ (bx) = a\text{Tr}(bx)$ for any $a, b \in \mathbb{F}_q^\times$. Thus the automorphism group of a spread set of $\mathbb{F}_q$ acts transitively on rank one matrices, as claimed.

\[\square\]

2.3. Tensors and Linear Codes. In this section we generalise Brockitt and Dobkin’s result from [4] to give $n$-dimensional $\mathbb{F}_q$-linear codes for concise 3-fold tensors over $\mathbb{F}_2$. The generalisation from concise 3-fold tensors over $\mathbb{F}_q$ is straightforward and can be found in Burgisser et al. [5, Theorem 18.4] where the result is rightfully attributed to Brockitt and Dobkin.

The result relates the tensor rank of a tensor $T$ to the minimum distance of certain linear block codes associated to $T$.

Consider a decomposition of a tensor $T \in \bigotimes_{i=1}^t V_i$ into the sum of $R$ pure tensors, say

\[T = \sum_{j=1}^R v_{j1} \otimes \cdots \otimes v_{jt}.\]

For $i \in \{1, \ldots, t\}$, define

\[G_i = \left( \begin{array}{c|c|\cdots|c} v_{i1}^T & v_{i2}^T & \cdots & v_{iR}^T \end{array} \right),\]

regarded as an $(\dim(V_i) \times R)$-matrix over $\mathbb{F}_q$. Denote the linear code generated by the rows of $G_i$ by $C_i$. Then $C_i$ is a linear code (in the Hamming metric) of length $R$ and dimension at most $\dim(V_i)$. The codewords of $C_i$ are of the form $(v^\vee(v_{i1}), v^\vee(v_{i2}), \ldots, v^\vee(v_{iR}))$ for some $v^\vee \in V_i^\vee$. Note that decompositions of a tensor are far from unique, and so these codes are not canonically defined by a tensor; rather, they are defined by a decomposition of a tensor.

Note that $\dim(C_i) = \dim(V_i)$ if and only if $T$ is $i$-concise; for the matrix $G_i$ does not have full row rank if and only if there exists $v^\vee \in V_i^\vee$ with $v^\vee(v_{ji}) = 0$ for all $j \in \{1, \ldots, R\}$, if and only if there exists $v^\vee \in V_i^\vee$ such that $v^\vee(T) = 0$, if and only if $T$ is not $i$-concise.

**Lemma 6.** For each $i \in \{1, \ldots, t\}$, the minimum distance of the code $C_i$ is at least the minimum tensor rank of a nonzero element of the $i$-th contraction space $C_i(T)$.

**Proof.** Consider an element $v^\vee \in V_i^\vee$, the corresponding contraction $v^\vee(T)$, and the corresponding codeword

\[c = (v^\vee(v_{i1}), v^\vee(v_{i2}), \ldots, v^\vee(v_{iR})).\]

Let $J \subset \{1, \ldots, R\}$ denote the support of $c$; that is, $J = \{j : v^\vee(v_{ji}) \neq 0\}$. Then

\[v^\vee(T) = \sum_{j \in J} v^\vee(v_{ji})(v_{j1} \otimes \cdots \otimes v_{ji-1} \otimes v_{ji+1} \otimes \cdots \otimes v_{jt}),\]

and so the tensor rank of $v^\vee(T)$ is at most $|J| = \text{wt}(c)$, implying the result. \[\square\]

A generally weaker but more easy to apply result is the following. We note that these two lemmas coincide in the case $t = 3$.

**Lemma 7.** For each $i \in \{1, \ldots, t\}$, the minimum distance of the code $C_i$ is at least

\[\min\{\max\{\dim(v^\vee(C_j(T))) : j \neq i\} : v^\vee \in V_i^\vee\}.\]

**Proof.** Let $v^\vee \in V_i^\vee$ and let $v_{ji}^\vee \in V_j^\vee$, and let $c$ be the codeword of $C_i$ corresponding to $v^\vee$. As in the proof of Lemma 6, $v^\vee(T)$ has tensor rank at most $\text{wt}(c)$, and so its contraction space $C_j(v^\vee(T))$ has dimension at most $\text{wt}(c)$. Then it is straightforward to verify that $C_j(v^\vee(T)) = v^\vee(C_j(T))$ by definition, proving the result. \[\square\]
The following theorem is a generalisation of a theorem, for concise 3-fold tensors, of Brockett and Dobkin [4], and Burgisser et al. [5, Theorem 18.4]. The theorem relates the tensor rank to the minimal length of a linear code with given dimension and minimum distance. We let $N_q(k, d)$ denote the shortest $\mathbb{F}_q$-linear code with dimension $k$ and minimum Hamming distance $d$.

**Theorem 2.** The tensor rank of a tensor $T$ is at least $N_q(\dim(C), d_i)$, for each $i \in \{1, \ldots, t\}$, where $d_i$ is the minimum tensor rank of an element of $C(t)$.

**Proof.** This follows immediately from Lemma 8 for if $T$ has tensor rank $R$, then $C_i$ is an $[R, \dim(C), d_i]$ code, and so $R \geq N_q(\dim(C), d_i)$ by definition. \qed

In the case of the tensor of a presemifield, we have that the dimension of $C_i$ is $n$, and every nonzero element of each contraction space is an invertible matrix, and hence $d_i \geq n$. Thus we obtain the following.

**Lemma 8.** The tensor rank of a presemifield of dimension $n$ over $\mathbb{F}_q$ is at least $N_q(n, n)$.

The following results are geared towards assisting with the algorithmic calculation of the tensor rank. Consider the following two sets associated with a minimal decomposition of $T$. Let

$$S = \{v_{j_1} \otimes \cdots \otimes v_{j_t} : j \in \{1, \ldots, R\}\},$$

where $T$ has rank $R$ and is the sum of the elements of $S$, and

$$S_i = \{v_{j_1} \otimes \cdots \otimes v_{j_i} \otimes v_{j,i+1} \otimes \cdots \otimes v_{j_t} : j \in \{1, \ldots, R\}\}.$$

**Lemma 9.** Let $d$ be such that there does not exist an $\mathbb{F}_q$-linear $[R, \dim(C), d + 1]$-code. Then the set $S_i$ contains a subset $U$ of size $d - 1$ such that the span $\langle U, C_i(T) \rangle$ contains at least one further element of $S_i$.

**Proof.** Let $c$ be a codeword of minimum weight $m$ in $C_i$, determined by $v^\vee \in V_i^\vee$. Then $m \leq d$ and $S_i$ contains a subset $W$ consisting of $m$ tensors whose span contains $v^\vee(T)$. Let $W' = W \setminus \{w\}$ for some $w \in W$, and let $U$ be the union of $W'$ and any $d - m$ elements of $S_i \setminus W$. Then $w \in \langle U, C_i(T) \rangle$, proving the claim. \qed

**Lemma 10.** Let $S$ be a semifield of order $q^n$ with a spread set $C$, and suppose the tensor rank of $S$ is $R$. If there does not exist an $[R, n, n + 1]$ code over $\mathbb{F}_q$, then there exists a $(2n - 1)$-dimensional subspace containing $C$ containing at least $n$ linearly independent elements of rank one.

**Proof.** This follows from Lemma 9 taking $d = n$, given that $\dim(C_i) = n$. Using the notation of that lemma, the space $\langle U \rangle$ is disjoint from $C$ as elements of $\langle U \rangle$ have rank at most $n - 1$, while nonzero elements of $C$ have rank $n$. Furthermore as the $n-1$ elements of $U$ and one further element $w$ of rank one span an element of $C$ of rank $n$, the elements of $U$ must be linearly independent. This shows that $\langle U, C_i(T) \rangle$ has dimension $2n - 1$. \qed

**Lemma 11.** If the tensor rank of a semifield of dimension $n$ over $\mathbb{F}_q$ is $R$, then for any $k \leq n$, its spread set contains a $(n - k)$-dimensional subspace of tensor rank at most $R - k$.

**Proof.** Suppose $C$ is a semifield spread set, contained in the span of the $R$ rank one matrices $A_1, \ldots, A_R$. Then the subspace $C \cap \langle A_1, \ldots, A_{R-k} \rangle$ has dimension $\geq n - k$, and has tensor rank at most $R - k$ by construction. \qed

2.4. Known Tensor Ranks. The following is well known.

**Lemma 12.** The tensor rank of the field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is at least $2n - 1$, with equality if and only if $q \geq 2n - 1$.

One direction of this result follows from Lemma 8 and the well-known results for $N_q(n, n)$, while the other direction follows from a direct construction of a tensor representing $\mathbb{F}_{q^n}$, obtained via polynomial interpolation [2]. It is known that the tensor rank of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is at most $C_q n$, where $C_q$ is a constant. Further bounds and asymptotic results for the tensor rank of $\mathbb{F}_{q^n}$ are known; we refer to for example [2] for further results in this direction. We detail one such result from [2] for context.
Lemma 13. The tensor rank of a field of dimension $n$ over $\mathbb{F}_2$ is at most
\[ \min\{38n, \frac{477}{26}n + \frac{45}{2}\} \].

In [14] the tensor ranks of some small presemifields were calculated precisely.

Lemma 14. The tensor rank of a semifield of order $2^3$ or $3^3$ is precisely 6.

This last two lemmas give the following.

Lemma 15. The tensor rank of a field of degree 3 over $\mathbb{F}_q$ is precisely 6 if $q \leq 3$, and precisely 5 if $q > 3$.

This leaves the smallest open cases to be those of presemifields of order $2^4, 2^5$, and $3^4$. In this paper we complete the first and third cases.

3. Algorithms

There are two main algorithms used in this work, denoted Algorithms 2 and 3 below. Algorithm 2 builds up subspaces of $M_n(\mathbb{F}_q)$ spanned by matrices of rank one, up to equivalence under the action of $G \cong \text{GL}(\mathbb{F}_q^n) \times \text{GL}(\mathbb{F}_q^n)$, and looks for semifield spread sets contained therein. Algorithm 3 begins with a semifield spread set, and adds in rank one matrices until the resulting space is spanned by the rank one elements contained in it, using the automorphism group of the semifield spread set at each step. Which of these algorithms is more appropriate for a particular case depends on the tensor rank (which we do not know a priori), and the size of the automorphism group of the spread set (which we do know). Algorithm 2 is the best option for low tensor rank and small automorphism group, whereas Algorithm 3 is the best option for high tensor rank and large automorphism group.

The two authors of this paper implemented the algorithms independently in two different systems (the FinInG package for GAP, and MAGMA, respectively). In GAP, equivalence was tested using group theoretic and finite geometry techniques. In MAGMA, equivalence was tested using linear algebraic techniques, using modifications of the algorithms presented in [20], [21]. We will refer to both of these algorithms as EquivalenceClasses, which takes as input a list of semifield spread sets (and an optional subgroup of $\text{GL}(\mathbb{F}_q^n) \times \text{GL}(\mathbb{F}_q^n)$), and returns a list of representatives for the distinct equivalence classes of the input.

We now give a conceptual description of these algorithms. The following notation is used. Let $e_1, \ldots, e_n$ be the standard basis for the vector space of $n \times 1$ matrices over $\mathbb{F}_q$. Define $\text{diag} = \langle e_i e_i^T : i \in \{1, \ldots, n\}\rangle$ as the space of diagonal matrices. Let $X$ denote the set of rank one matrices. If $a$ denotes a subspace of $M_n(\mathbb{F}_q)$ then $a^*$ denotes the set of nonzero elements of $a$.

3.1. Finding semifield spread sets in a given space. The first algorithm takes as input a subspace $S \leq M_n(\mathbb{F}_q)$ and finds all (semifield) spread sets contained in $S$.

Algorithm 1: SpreadSets
input a subspace $S \leq M_n(\mathbb{F}_q)$

(Step 1) $E_1 = \{a \in S : \det(a) \neq 0, a_1 = e_i\}$, where $a_1$ denotes the first row of $a$.
(Step 2) $A = \{\langle a \rangle : a \in E_1\}$, $m = 1$
(Step 3) $A = \{(a, b) : a \in A, b \in E_{m+1}\}$, $m = m + 1$
(Step 4) $A = \{a \in A : \forall x \in a^* \det(x) \neq 0\}$
(Step 5) if $m = n$ return $\text{SpreadSets}(S) := \text{EquivalenceClasses}(A)$
Otherwise repeat Steps 3-5.

3.2. Building spread sets of given tensor ranks. At each step we extend each subspace of $M_n(\mathbb{F}_q)$ with an element of rank one, calculate representatives for the equivalence classes, and calculate the spread sets contained in each representative.

Algorithm 2: SpreadSetsByRank
input an integer $R \geq n$
(Step 1) \( A = \{ \text{diag} \}, m = n. \)

(Step 2) \( A = \{ (a, b) : a \in A, b \in X, b \notin a \}, m = m + 1. \)

(Step 3) \( A = \text{EquivalenceClasses}(A) \)

(Step 4) \( SS_m = \cup_{a \in A} \text{SpreadSets}(a) \)

(Step 5) if \( m = R \) return \( \text{SpreadSetsByRank}(R) := \text{EquivalenceClasses}(SS_m) \)

Otherwise repeat Steps 2-5.

The output contains representatives for all isomorphism classes of semifields of tensor rank at most \( R. \)

3.3. Calculating the tensor rank of a given semifield spread set. This algorithm can be used to verify the tensor rank of a given spread set \( C. \)

Algorithm 3: \textbf{TensorRank}

\textbf{input} a spread set \( C \leq M_n(\mathbb{F}_q) \) with automorphism group \( G_C. \)

(Step 1) \( A = \{ C \}, m = n \)

(Step 2) \( A = \{ (a, b) : a \in A, b \in X, b \notin a \}, m = m + 1. \)

(Step 3) If \( \exists a \in A \) such that \( \langle x \in a : \text{rank}(x) = 1 \rangle = a \) then return \( \text{TensorRank}(C) := m. \)

Otherwise \( A = \text{EquivalenceClasses}(A, G_C); \) repeat Step 2.

\textbf{Notation.} We will sometimes use a more concise representation for a matrices in \( M_n(\mathbb{F}_p) \) and write

\[ \sum_{i,j} a_{ij}p^{(i-1)n+(j-1)} \]

for a matrix with \( (i, j) \)-entry \( a_{ij}. \)

4. SEMIFIELDS OF ORDER \( 2^4 \)

There are 3 isomorphism classes of semifields of order \( 2^4 \), falling into 3 Knuth orbits. These were first classified by Knuth [12]. We denote them by \( \mathbb{F}_{2^4}, \mathcal{S}_1, \) and \( \mathcal{S}_2, \) where \( \mathcal{S}_1 \) is the unique semifield of order \( 2^4 \) containing a nucleus of order \( 2^2 \).

The following result was noted in [6], based on computer classifications by the second author of this paper. It was calculated using the above algorithms, and we present proof below. It was further noted in [6] that a spread set of the field \( \mathbb{F}_{2^4} \) contains no hyperplane (three-dimensional subspace) with tensor rank 7, whereas the spread sets of the other two classes of semifields do possess hyperplanes with tensor rank 7.

Theorem 3. \textit{The tensor rank of every semifield of order \( 2^4 \) is nine.}

\textbf{Proof.} By Lemma [8] any semifield of order \( 2^4 \) has tensor rank at least eight, as \( N_2(4, 4) = 8 [9]. \)

We utilise the algorithm in Section [8]. We retain only the six-dimensional spaces containing a partial spread set of dimension two, and only the seven-dimensional spaces containing a partial spread set of dimension three. This ensures that we obtain a representative for every semifield of tensor rank eight, should one exist.

We find 19 equivalence classes of five-dimensional spaces spanned by rank one matrices. To representatives of these classes we add each matrix of rank one and classify them up to equivalence, finding 236 equivalence classes of six-dimensional spaces. Of these, 33 contained a partial spread set of dimension 2; we retain these 33 representatives and discard the rest. To each of these representatives we add each rank one matrix, finding 4371 seven-dimensional spaces forming 910 equivalence classes. Of these only two contain a partial spread set of dimension 3; again we discard the rest. To each of these two representatives we add each rank one matrix, finding 201 eight-dimensional spaces forming 23 equivalence classes. None of these contain a spread set, proving that the tensor rank of any semifield of order \( 2^4 \) is at least nine.

Thus it suffices to show that a spread set for each is contained in a space spanned by nine matrices of rank one.
The following are representations of bases of a spread set of each semifield.

\[
\begin{array}{cccc}
F_{2^4} & 33825 & 14402 & 25476 & 50744 \\
\mathcal{S}_1 & 33825 & 51250 & 63940 & 24136 \\
\mathcal{S}_2 & 33825 & 22594 & 11684 & 51864
\end{array}
\]

A computer calculation implementing Algorithm 2 showed that each of these spread sets is indeed contained in a space spanned by nine matrices of rank one. The nine rank one matrices spanning each spread set are as follows.

\[
\begin{array}{cccc}
\mathcal{F}_{2^4} & 85 & 8738 & 57582 & 32896 & 1632 & 3072 & 30576 & 53261 & 4096 \\
\mathcal{S}_1 & 4112 & 238 & 80 & 53469 & 4353 & 2304 & 13059 & 2570 & 26112 \\
\mathcal{S}_2 & 1 & 204 & 35469 & 39321 & 4080 & 2048 & 43530 & 47872 & 57344
\end{array}
\]

Thus each semifield of order \(2^4\) has rank nine, as claimed. □

Expanded details of these facts can be found in the next sections. We note that these sets of rank one matrices are not unique, even up to equivalence. For example, there are five equivalence classes of nine-dimensional spaces spanned by rank one matrices containing the spread set of \(F_{16}\). The chosen decompositions are arbitrary.

4.1. The field \(F_{2^4}\). A basis for a spread set for the field \(F_{2^4}\) is

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1
\end{pmatrix}
\]

This is contained in the space spanned by the following nine rank one matrices.

\[
\begin{array}{cccc}
\begin{pmatrix}
1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\end{array}
\]

4.2. The semifield \(\mathcal{S}_1\) of order \(2^4\) with a nucleus of order \(2^2\). The semifield with basis

\[
\begin{array}{cccc}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{array},
\begin{array}{cccc}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1
\end{array},
\begin{array}{cccc}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1
\end{array},
\begin{array}{cccc}
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0
\end{array}
\]

is spanned by the following nine rank one matrices:

\[
\begin{array}{cccc}
\begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0
\end{pmatrix},
\end{array}
\]

\[
\begin{array}{cccc}
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0
\end{pmatrix},
\end{array}
\]

\[
\begin{array}{cccc}
\begin{pmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1
\end{pmatrix},
\begin{pmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1
\end{pmatrix},
\end{array}
\]

9
4.3. The semifield $\mathcal{S}_2$ of order $2^4$ with trivial nuclei. The semifield with basis

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1
\end{bmatrix}
\]

is spanned by the following nine rank one matrices:

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1
\end{bmatrix}
\]

5. Semifields of order $3^4$

There are 27 isomorphism classes of semifields of order $3^4$, falling into 12 Knuth orbits. These were first classified by Dempwolff [4], who labelled the Knuth orbits as I-XII.

By Lemma 8 any semifield has tensor rank at least eight, as $N_3(4, 4) = 8 [9]$. As we will see in the forthcoming sections, the tensor rank of these semifields is either 8 or 9. This is the first result establishing the fact that two semifields of the same order can have different tensor rank. This shows that the tensor rank of a semifield is a non-trivial invariant for finite semifields. It also shows that from a computational point of view, for a fixed order, certain semifields will perform better than others. In fact, it turns out that the finite field and the GTF of order $3^4$ are the worst choices in terms of complexity of multiplication, since they both have tensor rank 9, while the other semifields of order $3^4$ have tensor rank 8.

5.1. The field $\mathbb{F}_{3^4}$. This is labelled as XII in [4]. We choose a different basis for convenience. A basis for a spread set of $\mathbb{F}_{3^4}$ is the following:

\[
\begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0
\end{bmatrix}
\]

Lemma 16. The tensor rank of $\mathbb{F}_{3^4}$ is at least nine.

Proof. Let $\mathcal{C}$ be a spread set for $\mathbb{F}_{3^4}$. By Lemma 11 if $\mathbb{F}_{3^4}$ has tensor rank eight, then since there does not exist an [8, 4, 5] code over $\mathbb{F}_3$, there must exist three elements $A_1, A_2, A_3$ of $M_4(\mathbb{F}_3)$ of rank one such that $\langle \mathcal{C}, A_1, A_2, A_3 \rangle$ contains an element of rank one which linearly independent from $A_1, A_2, A_3$.

Since the automorphism group of $\mathcal{C}$ acts transitively on matrices of rank one, we may choose $A_1$. We calculate the orbits of rank one matrices under the automorphism group of $\langle \mathcal{C}, A_1 \rangle$ and form representatives for the six-dimensional spaces spanned by $\mathcal{C}$ and two matrices of rank one; we find that there are 662 of these in total. We then form all seven-dimensional spaces spanned by one of these representatives and another matrix of rank one; we find 763858 spaces.

By the above, we may discard any of these spaces which do not contain four linearly independent matrices of rank one. We are left with 5078 spaces. For each of these we form all eight-dimensional spaces containing one of these spaces and another matrix of rank one. We find that none of these spaces contain eight linearly independent matrices of rank one, proving that the tensor rank of $\mathbb{F}_{3^4}$ is at least nine.

$\square$

Theorem 4. The tensor rank of $\mathbb{F}_{3^4}$ is exactly nine.
Proof. By Lemma 16, the tensor rank of $\mathbb{F}_3^4$ is at least nine. Thus it suffices to show that the spread set of $\mathbb{F}_3^4$ is contained in a space spanned by nine matrices of rank one.

One verifies that the spread set for $\mathbb{F}_3^4$ is contained in the space spanned by the following nine matrices of rank one.

\[
\begin{align*}
&\begin{pmatrix}
1 & 0 & 0 & 2 \\
2 & 0 & 0 & 1 \\
1 & 0 & 0 & 2 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 2 & 2 & 1 \\
2 & 1 & 1 & 2 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 \\
1 & 2 & 1 & 0 \\
2 & 1 & 2 & 0
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
2 & 2 & 2 & 2 \\
2 & 2 & 1 & 1 \\
0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 & 2 \\
0 & 1 & 0 & 2 \\
0 & 2 & 0 & 1 \\
0 & 0 & 0 & 0
\end{pmatrix}
\end{align*}
\]

□

As seen in Section 2.3, a minimal decomposition of a tensor $T$ of tensor rank $R$ gives three linear codes. The three $n \times R$ matrices $G_1, G_2, G_3$ whose rows generate the linear codes $C_1, C_2, C_3$, obtained from the decomposition implied by the matrices in the proof of Lemma 4, are as follows.

\[
G_1 = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
2 & 2 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 2 & 1 & 1 & 2 \\
0 & 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0
\end{pmatrix}
\]

\[
G_2 = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 2 & 1 & 0 & 1 & 1 \\
0 & 2 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
2 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 2
\end{pmatrix}
\]

\[
G_3 = \begin{pmatrix}
2 & 2 & 1 & 2 & 1 & 2 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 2 & 0 & 0 & 0 \\
2 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 1 \\
2 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0
\end{pmatrix}
\]

We note that each of these is a generator matrix for a $[9, 4, 4]_3$ code. It can be verified that the first two are equivalent to each other. However, the third is inequivalent to the first two. This can easily be verified by computing the weight distribution of the codes which give $[1, 0, 0, 0, 6, 24, 24, 12, 12, 2]$ for $G_1$ and $[1, 0, 0, 0, 10, 22, 22, 8, 14, 4]$ for $G_3$.

Finally, we remark that the minimal decomposition given in the proof of Lemma 4 is far from unique. This implies that there are many other triples of linear codes associated to a minimal decomposition of the tensor of $\mathbb{F}_3^4$.

5.2. The Generalised Twisted Field of order $3^4$. This is labelled as IX in [7]. We choose a different basis for convenience, and denote it as GTF$_{3^4}$. A basis for a spread set of a generalised twisted field of order $3^4$ is the following.

\[
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 1 & 1 \\ 2 & 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 0 & 2 & 1 \\ 0 & 2 & 1 & 0 \end{pmatrix}
\]

Lemma 17. The tensor rank of GTF$_{3^4}$ is at least nine.
Proof. This result uses the same approach as Lemma 16, taking into account that the automorphism group of a spread set for $GTF_{3^4}$ is smaller than that of a spread set for $F_{3^4}$. We get ten equivalence classes of five-dimensional spaces, 15425 six-dimensional spaces, and 11236916 seven-dimensional spaces.

Of these, 62649 contain four linearly independent elements of rank one. There are 82422491 eight-dimensional spaces spanned by one of these spaces and an element of rank one; none of which are spanned by eight rank one.

□

Theorem 5. The tensor rank of $GTF_{3^4}$ is exactly nine.

Proof. By Lemma 17, the tensor rank of $GTF_{3^4}$ is at least nine. Thus it suffices to verify that the spread set for $GTF_{3^4}$ is contained in the space spanned by the following nine matrices of rank one.

\[
\begin{pmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 2 & 1 \\
1 & 1 & 2 & 2 \\
0 & 0 & 0 & 0 \\
1 & 2 & 1 & 1
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 & 0 \\
1 & 2 & 1 & 1 \\
1 & 2 & 1 & 1 \\
0 & 0 & 0 & 0
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 1 & 2 \\
1 & 2 & 0 & 1 \\
1 & 0 & 1 & 2 \\
1 & 0 & 1 & 2
\end{pmatrix},
\begin{pmatrix}
2 & 0 & 2 & 1 \\
1 & 0 & 1 & 2 \\
1 & 0 & 1 & 2 \\
1 & 0 & 1 & 2
\end{pmatrix}
\]

The more concise representation of the bases of a spread set for the field and generalized twisted field are tabulated here.

\begin{center}
\begin{tabular}{c|cccc}
 & $F_{3^4}$ & $GTF_{3^4}$ \\
\hline
$1$ & 14408200 & 14408200 \\
$2$ & 15058227 & 37463637 \\
$3$ & 16660575 & 34827984 \\
$4$ & 21463326 & 8282925 \\
\end{tabular}
\end{center}

The more concise representation of the set of nine rank one matrices spanning the above spread sets are tabulated here.

\begin{center}
\begin{tabular}{c|cccc}
 & $F_{3^4}$ & $GTF_{3^4}$ \\
\hline
$1$ & 363259 & 14528241 \\
$2$ & 5560 & 426511 \\
$3$ & 38502864 & 40395672 \\
$4$ & 59787 & 1614006 \\
$5$ & 21785760 & 221187 \\
\end{tabular}
\end{center}

5.3. The remaining semifields of order $3^4$. The following are bases for representatives for the set of Knuth orbits of the remaining semifields of order $3^4$. The numbering is taken from [7], though different bases are chosen for convenience.

\begin{center}
\begin{tabular}{c|cccc}
 & $I$ & $II$ & $III$ & $IV$ \\
\hline
$V$ & 512735 & 4604203 & 14467492 & 19878561 \\
$VI$ & 8168391 & 15640965 & 14958678 & 24409758 \\
$VII$ & 10127682 & 26024736 & 39188133 & 35533648 \\
$VIII$ & 27851041 & 26930970 & 42832017 & 42221016 \\
$IX$ & 14408200 & 26024736 & 39188133 & 24409758 \\
$X$ & 10127682 & 26024736 & 39188133 & 24409758 \\
$XI$ & 27851041 & 26930970 & 42832017 & 42221016 \\
\end{tabular}
\end{center}

Lemma 18. All semifields from the families $I$-$VIII$ and $X$-$XI$ have tensor rank eight.
Proof. By Lemma 8, the tensor rank of each of these semifields is at least eight. One verifies that the spread sets are contained in the space spanned by the eight matrices of rank one as listed below, thus proving that the tensor rank is precisely eight.

The algorithm used for Lemmas 16 and 17 are not efficient here, as the automorphism groups are much smaller. Instead we utilise the algorithm in Section 3.2. We retain only the six-dimensional spaces containing a partial spread set of dimension two, and only the seven-dimensional spaces containing a partial spread set of dimension three. This ensures that we obtain a representative for every semifield of tensor rank eight.

We found that each spread set is contained in the span of the four elementary diagonal matrices, represented by 1, 243, 59049, 14348907, and four further rank one matrices noted in the below table.

\[
\begin{array}{lllll}
I & 285649 & 13819585 & 25824144 & 42259239 \\
II & 18834768 & 20729397 & 25402879 & 28081132 \\
III & 325507 & 7442224 & 18834768 & 20982117 \\
IV & 9035896 & 18981031 & 39280132 & 41711436 \\
V & 285649 & 13819585 & 25824144 & 42259239 \\
VI & 285649 & 13819585 & 25824144 & 42259239 \\
VII & 325507 & 18834768 & 34325839 & 41964195 \\
VIII & 12329415 & 18981031 & 39280132 & 42518560 \\
IX & 423775 & 13288075 & 18981031 & 21520120 \\
XI & 9035896 & 18981031 & 23363440 & 39280132 \\
\end{array}
\]

Remark 1. Note that we did not know a priori which semifields would have tensor rank eight. If a semifield other than the field or twisted field would have been found to have had tensor rank greater than eight, it would have taken significantly longer to calculate its tensor rank, as the automorphism groups are much smaller than those of the field and generalised twisted field.

We note that there are subspaces spanned by eight rank one matrices containing many isotopism classes of semifields of order $3^4$. The maximum is ten; that is, there exists an eight dimensional space spanned by rank ones which contains semifield spread sets in 10 of the 27 isotopism classes (and five of the 10 Knuth orbits).

6. Conclusion and Future Work

In the first part of the paper we generalised a well known result of Brockett and Dobkin, which gives a relation between the rank of a concise 3-fold tensor and the minimal length of certain linear codes, to $t$-fold tensors without the condition of conciseness. In the second part of the paper we determined the tensor rank of all semifields of order 16 over $\mathbb{F}_2$ and of order 81 over $\mathbb{F}_3$. All semifields of order 16 have tensor rank nine over $\mathbb{F}_2$. Our results for order 81 establish the tensor rank of semifields as a nontrivial invariant of the isotopism classes of semifields (and of the Knuth orbit). This provides the first proof for the existence of semifields of the same order with different tensor rank. All semifields of order 81 have tensor rank eight over $\mathbb{F}_3$, except for the finite field $\mathbb{F}_{81}$ and the generalized twisted field of order 81, which both have rank nine over $\mathbb{F}_3$.

As a consequence of the relation between the tensor rank and the multiplicative complexity, the lower tensor rank of some semifields compared to fields of the same order imply that some semifields are more efficient than finite fields in terms of algebra operations. As many applications of finite fields require extension field operations performed as efficiently as possible, it may be beneficial to instead use a semifield of lower tensor rank, should the property of multiplicative associativity not be crucial to the application. Towards this goal, further results on the tensor rank of semifields over $\mathbb{F}_2$ in particular are required.

Further future work may involve analysis of the different minimal tensor decompositions for a given semifield, in particular with regard to which linear codes can (or cannot) appear.
References

[1] Albert, A. A.: Generalized twisted fields, Pacific J. Math. 11 (1961), 1-8.
[2] Ballet, S.; Pieltant, J.: On the tensor rank of multiplication in any extension of $\mathbb{F}_2$, Journal of Complexity 27 (2011) 230–245.
[3] Bremner, M.R., Stavrou, S.G.: Canonical forms of $2 \times 2 \times 2$ and $2 \times 2 \times 2 \times 2$ arrays over $\mathbb{F}_2$ and $\mathbb{F}_3$, Linear and Multilinear Algebra 61 (2013), 986-997.
[4] Brockett, R. W., Dobkin, D.: On the Optimal Evaluation of a Set of Bilinear Forms, Lin. Algebra Apl., 19 (1978) 207-235.
[5] Bürgisser, P., Clausen, M., Shokrollahi, M.A.: Algebraic Complexity Theory, Grundlehren der mathematischen Wissenschaftern 315, Springer, 1997.
[6] Byrne, E., Neri, A., Ravagnani, A., Sheekey, J.: Tensor Representation of Rank-Metric Codes, SIAM Journal on Applied Algebra and Geometry, to appear.
[7] Dempwolff, U.: Semifield planes of order 81, J. Geom. 89 (2008), 1-16.
[8] Dickson, L. E.; On finite algebras, Nachrichten der Gesellschaften der Wissenschaften zu Göttingen (1905) 358-393.
[9] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available http://www.codetables.de/
[10] Grochow, J.A., Qiao, Y.: Isomorphism problems for tensors, groups, and cubic forms: completeness and reductions, arxiv:1907.00309.
[11] Håstad, J.: Tensor rank is NP-complete. J. Algorithms 11 (1990), no. 4, 644–654.
[12] Knuth, D. E.: Finite semifields and projective planes. J. Algebra 2 (1965) 182-217.
[13] Lavrauw, M.: Finite semifields and nonsingular tensors, Des. Codes Cryptogr. 68 (2013), 205-227.
[14] Lavrauw, M., Pavan, A., Zanella, C.: On the rank of $3 \times 3 \times 3$-tensors, Linear and Multilinear Algebra 61 (2013) 648–652, 2013.
[15] Lavrauw, M.; Polverino, O.: Finite Semifields. Chapter in Current research topics in Galois geometries. Nova Academic Publishers (J. De Beule and L. Storme, Eds.).
[16] Lavrauw, M.; Rodgers, M.: Classification of 8-dimensional rank two commutative semifields. Adv. Geom. 19 (2019), no. 1, 57–64.
[17] Lavrauw, M., Sheekey, J.: Orbits of the stabiliser group of the Segre variety product of three projective lines, Finite Fields Appl. 26 (2014) 1–6.
[18] Lavrauw, M., Sheekey, J.: Commutative semifields of order 2401. In preparation.
[19] Liebler, R.A.: On nonsingular tensors and related projective planes, Geom. Dedicata 11 (1981) 455–464.
[20] Rúa, I.F., Combarro, E.F., Ranilla, J.: Classification of semifields of order 64, J. Algebra 322 (2009) 4011-4029.
[21] Rúa, I.F., Combarro, E.F., Ranilla, J.: New advances in the computational exploration of semifields, Int. J. Comput. Math. 88 (2011) 1990-2000.
[22] Stavrou, S.G.: Canonical forms of $2 \times 2 \times 2$ and $2 \times 2 \times 2 \times 2$ symmetric tensors over prime fields, Linear Multilinear Algebra 62 (2014) 1169–1186.