On the generalized distributive set of a finite nearfield

Prudence Djagba

Department of Mathematical Sciences, Stellenbosch University, South Africa
e-mail: prudence@aims.ac.za

Abstract: For any nearfield \((R, +, \circ)\), denote by \(D(R)\) the set of all distributive elements of \(R\). Let \(R\) be a finite Dickson nearfield that arises from Dickson pair \((q, n)\). For a given pair \((\alpha, \beta)\) we study the generalized distributive set \(D(\alpha, \beta) = \{\lambda \in R \mid (\alpha + \beta) \circ \lambda = \alpha \circ \lambda \circ \beta \circ \lambda\}\) where \(\circ\) is the multiplication of the Dickson nearfield. We find that \(D(\alpha, \beta)\) is not in general a subfield of the finite field \(\mathbb{F}_{q^n}\). In contrast to the situation for \(D(R)\), we also find that \(D(\alpha, \beta)\) is not in general a subnearfield of \(R\). We obtain sufficient conditions on \(\alpha, \beta\) for \(D(\alpha, \beta)\) to be a subfield of \(\mathbb{F}_{q^n}\) and derive an algorithm that tests if \(D(\alpha, \beta)\) is a subfield of \(\mathbb{F}_{q^n}\) or not. We also study the notions of \(R\)-dimension, \(R\)-basis, seed sets and seed number of \(R\)-subgroups of the Beidleman near-vector spaces \(R^m\) where \(m\) is a positive integer. Finally we determine the maximal \(R\)-dimension of \(\text{gen}(v_1, v_2)\) for \(v_1, v_2 \in R^m\), where \(\text{gen}(v_1, v_2)\) is the smallest \(R\)-subgroup containing the vectors \(v_1\) and \(v_2\).

Keywords: Dickson nearfields, Beidleman near-vector spaces, \(R\)-subgroups, generalized distributive set.

2010 MSC: 16Y30;12K05

1 Introduction and preliminaries

In 1905 Dickson wanted to know what structure arises if one axiom in the list of axioms for skewfields was weakened. He found that there exist “nearfields”, which fulfill all axioms for skewfields except one distributive law. Dickson achieved this by starting with a field and changing the multiplication into a new operation [5]. Thirty years later Zassenhaus classified all the finite nearfields in [15]. He found that all finite nearfields are either finite Dickson nearfields or one of the seven exceptional types. Since then Dancs [8, 9], Karzel and Ellers [6], Zemmer [16] have solved some important problems in this area.

In 1996 the first notion of near-vector spaces was introduced by Beidleman [2] in his PhD thesis. This notion generalises and extends the concept of a vector space to obtain a certain structure which is no longer linear. He used nearring modules in the construction. Later André [1] introduced another notion of near-vector spaces and used automorphisms in the construction. André’s version has been studied in many papers, and theses, for example [10] while Beidleman near-vector spaces had not since his thesis until recently the authors of [4] added to the body of existing work.

In [4], the authors characterized the \(R\)-subgroups and subspaces of finite dimensional Beidleman near-vector spaces. In this paper we continue the work of that paper. We introduce the notion of \(R\)-dimension, \(R\)-basis, seed set and seed number of an \(R\)-subgroup and find some properties.

This paper is organized as follows. In subsection 1.1 we have used the results by Hull and Dobell ([11]) to explain the finite Dickson construction. In section 2 we recall some results from [4] characterizing the \(R\)-subgroups of \(R^m\). We attempt to give sufficient background for the paper because of the nearfield experts that are new
to finite dimensional Beidleman near-vector spaces. In section 3 we determine the distributive structure of finite Dickson nearfields. In section 4 we give an application of the distributive elements to the concept of $R$-subgroups of $R^m$ where $R$ is a finite nearfield and $m$ is a positive integer. We evaluate the possible values of $R$-dimension for a given value of seed number and determine the seed number of $R^m$ where $m$ is a positive integer such that $m \leq |R| + 1$.

1.1 Some remarks on finite nearfields

Let $S$ be any group with identity $0$. We will use $S^*$ to denote $S \setminus \{0\}$.

**Definition 1.1.** ([13]) Let $(R, +, \cdot)$ be a triple such that $(R, +)$ is a group, $(R, \cdot)$ is a semigroup, and $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$. Then $(R, +, \cdot)$ is a (left) nearring. If in addition $(R^*, \cdot)$ is a group then $(R, +, \cdot)$ is called a nearfield.

So a nearfield is an algebraic structure similar to a skewfield (sometimes called a division ring) except that it has only one of the two distributive laws. It is well known that the additive group of a (left) nearfield is abelian, see for instance [13]. Throughout this paper we will make use of (left) nearfields. To construct finite Dickson nearfields, we need two concepts: Dickson pair and coupling map.

**Definition 1.2.** ([13]) A pair of positive integers $(q, n)$ is called a Dickson pair if the following conditions are satisfied:

(i) $q$ is some power $p^l$ of some prime $p$,
(ii) each prime divisor of $n$ divides $q - 1$,
(iii) $q \equiv 3 \mod 4$ implies $4$ does not divide $n$.

**Example 1.3.** The following are Dickson pairs: $(7, 9), (3, 2), (4, 3), (5, 4)$ and $(5, 8)$.

Let $(q, n)$ is a Dickson pair and $k \in \{1, \ldots, n\}$. We will denote the positive integer $q^{k-1} \mod q$ by $[k]_q$.

**Definition 1.4.** ([13]) Let $R$ be a nearfield and $\text{Aut}(R, +, \cdot)$ the set of all automorphisms of $R$. A map $\phi : R^* \to \text{Aut}(R, +, \cdot)$ defined by $n \mapsto \phi_n$ is called a coupling map if for all $n, m \in R^*$, $\phi_n \circ \phi_m = \phi_{\phi_n(m)n}$.

Furthermore, to generate a sequence of numbers which at least appear to be drawn at random from a certain probability distribution (uniform or normal, poisson, or some other), we begin with a positive integer $m$, called the modulus, a positive integer $x_0$, called starting value such that $0 \leq x_0 < m$, an integer $a$, called the multiplier such that $0 < a < m$ and another integer $c$, called the increment such that $0 \leq c < m$. We then define a sequence \{x_i\} of positive integers, each less than $m$, by means of the congruence relation

$$x_i \equiv (ax_{i-1} + c) \mod m. \quad (1)$$

For the case $c \neq 0$, an important number theoretic property has been discovered by Hull and Dobell in 1962 and is stated as the following:

**Theorem 1.5.** ([11]) The sequence defined by the congruence relation (1) has full period $m$, provided that

(i) $c$ is relatively prime to $m$,
(ii) \(a \equiv 1 \mod p\) if \(p\) is a prime factor of \(m\),
(iii) \(a \equiv 1 \mod 4\) if \(4\) is a factor of \(m\).

We now deduce the following well known result as a special case of Hull and Dobell’s theorem.

**Lemma 1.6.** ([13] [14]) Let \((q,n)\) be a Dickson pair. Then \([k]_q : 1 \leq k \leq n\) forms a finite complete set of different residues modulo \(n\).

**Proof.** We take \(x_0 = 1\), \(a = q\), \(m = n\) and \(c = 1\) into the relation (11) and apply Theorem 1.5. Thus we have the following: \(x_0 = 1, x_1 = q + 1, x_2 = q^2 + q + 1, \ldots, x_{n-1} = q^{n-1} + q^{n-2} + \ldots + 1\). Hence the sequence \(\{x_i\}_{i=0,\ldots,n-1}\) has full period \(n\) and are all different residues modulo \(n\). Thus \(\{x_0, \ldots, x_{n-1}\}\) is \([k]_q : 1 \leq k \leq n\). \(\square\)

Every Dickson pair \((q,n)\) gives rise to a finite Dickson nearfield. This is obtained by replacing the usual multiplication “*” in the finite field \(\mathbb{F}_{q^n}\) of order \(q^n\) with a new multiplication “◦”. We shall denote the set of Dickson nearfields arising from the Dickson pair \((q,n)\) by \(DN(q,n)\) and the Dickson nearfield arising from the Dickson pair \((q,n)\) with generator \(g\) by \(DN_g(q,n)\). Furthermore in [13] the new multiplication is constructed as follows:

Let \(g\) be such that \(\mathbb{F}_{q^n}^* = \langle g \rangle\) and \(H = \langle g^n \rangle\). The quotient group is given by

\[
\mathbb{F}_{q^n}^*/H = \{g^{[1]}H, g^{[2]}H, \ldots, g^{[n]}H\} = \{H, gH, \ldots, g^{n-1}H\}\]

by Lemma 1.6.

The coupling map \(\phi\) is defined as

\[
\mathbb{F}_{q^n}^* \rightarrow Aut(\mathbb{F}_{q^n}, +, \cdot) \\
\alpha \mapsto \phi_\alpha = \varphi^k(\alpha)
\]

where \(\varphi\) is the Frobenius automorphism of \(\mathbb{F}_{q^n}\) and \(k\) is a positive integer \((k \in \{1, \ldots, n\})\) such that \(\alpha \in g^{[k]}H\). Let \(\alpha, \beta \in \mathbb{F}_{q^n}\), the we have

\[
\alpha \circ \beta = \begin{cases} 
\alpha \cdot \phi_\alpha(\beta) & \text{if } \alpha \neq 0 \\
0 & \text{if } \alpha = 0
\end{cases}
\]

\[
= \begin{cases} 
\alpha \cdot \varphi^k(\beta) & \text{if } \alpha \in g^{[k]}H \\
0 & \text{if } \alpha = 0
\end{cases}
\]

\[
= \begin{cases} 
\alpha \cdot \beta^k & \text{if } \alpha \in g^{[k]}H \\
0 & \text{if } \alpha = 0
\end{cases}
\]

for \(k \in \{1, \ldots, n\}\). Thus \(DN_g(q,n) := (\mathbb{F}_{q^n}, +, \circ)\) is the finite Dickson nearfield constructed by taking \(H = \langle g^n \rangle\). By taking all Dickson pairs, all finite Dickson nearfields arise in this way. Furthermore we deduce the following.

**Lemma 1.7.** Let \((q,n)\) be a Dickson pair with \(q = p^l\) for some prime \(p\) and positive integers \(l,n\). Let \(g\) be a generator of \(\mathbb{F}_{q^n}\), and \(R\) the finite nearfield constructed with \(H = \langle g^n \rangle\). If \(n\) divides \(q-1\) then \(g^{[i]}H = g^iH\) for all \(i = 1, \ldots, n\).

**Proof.** Suppose that \(n\) divides \(q-1\). We need to show that \([i]_q \equiv i \mod n\) and we proceed by induction. For \(i = 1\). We have \([1]_q \equiv 1 \mod n\). Suppose that \([i]_q \equiv i \mod n\). Since \(n\) divides \(q-1\) then \(q^i \equiv 1 \mod n\). So \([i+1]_q \equiv i+1 \mod n\). \(\square\)
Note that the conclusion of Lemma 1.7 is not always true for any Dickson pair, for example, take \((q, n) = (7, 9)\). We have \([2]_7 = 8\) but 8 is not congruent to 2 modulo 9. The use of Theorem 1.5 taken from [11] allows us to give an alternate proof to that found in [14] of the following lemma.

**Lemma 1.8.** ([14]) Let \((q, n)\) be a Dickson pair with \(q = p^l\) for some prime \(p\) and positive integers \(l, n\). Let \(g\) be a generator of \(\mathbb{F}_q^*\) and \(R\) the finite nearfield constructed with \(H = \langle g^n \rangle\). Then \(n\) divides \([n]_q\) and \(g^{[n]_q} H = H\).

**Proof.** Suppose that \((q, n)\) is a Dickson pair. Let us consider \(x_0 = 1, a = q, m = n\) and \(c = 1\). By Theorem 1.5 the period of the sequence \(\{x_i\}\) is exactly \(n\). Thus \(1 = x_0\) and is equivalent to \(x_n\). But we have \(x_n - 1 = [n]_q\) which satisfies the recurrence

\[
x_n \equiv qx_{n-1} + 1 \mod n \iff 1 \equiv qx_{n-1} + 1 \mod n \iff qx_{n-1} \equiv 0 \mod n.
\]

Since every prime divisor of \(n\) divides \(q\) then \(\gcd(q, n) = 1\). Thus

\[
qx_{n-1} \equiv 0 \mod n \iff x_{n-1} \equiv 0 \mod n.
\]

Since \(n\) divides \([n]_q\) then \(g^{[n]_q} H = H\).

Thirty years after Dickson’s work, Zassenhaus fundamentally determined all finite nearfields.

**Theorem 1.9.** ([15]) A finite nearfield is either a finite Dickson nearfield or it is one of the 7 exceptional nearfields of order \(5^2, 7^2, 11^2, 23^2, 29^2, 59^2\).

Note that there exist two exceptional nearfields of order 11\(^2\) (see [15] for more details).

### 1.2 Beidleman near-vector spaces

The concept of a ring module can also be extended to a more general concept called a nearring module where the set of scalars is taken to be a nearring.

**Definition 1.10.** An additive group \((M, +)\) is called a (right) nearring module over a (left) nearring \(R\) if there exists a mapping,

\[
\eta : M \times R \to M
\]

\[
(m, r) \mapsto mr
\]

such that \(m(r_1 + r_2) = mr_1 + mr_2\) and \(m(r_1 r_2) = (mr_1) r_2\) for all \(r_1, r_2 \in R\) and \(m \in M\).

We write \(M_R\) to denote that \(M\) is a (right) nearring module over a (left) nearring \(R\).

**Definition 1.11.** ([2]) A subset \(H\) of a nearring module \(M_R\) is called an \(R\)-subgroup if \(H\) is a subgroup of \((M, +)\) and \(HR = \{hr | h \in H, r \in R\} \subseteq H\).

**Definition 1.12.** ([2]) A nearring module \(M_R\) is said to be irreducible if \(M_R\) contains no proper \(R\)-subgroups. In other words, the only \(R\)-subgroups of \(M_R\) are \(M_R\) and \(\{0\}\).

**Definition 1.13.** ([2]) Let \(M_R\) be a nearring module. \(N\) is a submodule of \(M_R\) if
(i) \((N, +)\) is a normal subgroup of \((M, +)\),
(ii) \((m + n)r - mr \in N\) for all \(m \in M, n \in N\) and \(r \in R\).

**Proposition 1.14.** (2) Let \(N\) be a submodule of \(M_R\). Then \(N\) is an \(R\)-subgroup of \(M_R\).

Note that the converse of this proposition is not true in general. In his thesis Beidleman gives a counter example.

**Theorem 1.15.** (2) Let \(R\) be a nearring that contains the identity element \(1 \neq 0\). \(R\) is a nearfield if and only if \(R\) contains no proper \(R\)-subgroups.

**Remark 1.16.** Let \(R\) be a nearfield. By Theorem 1.15, \(R\) is an irreducible \(R\)-module. Thus \(R\) contains only \(\{0\}\) and \(R\) as submodules of \(R\).

In the following, let \(\{M_i\}_{i \in I}\) be a collection of submodules of the nearring module \(M_R\).

**Definition 1.17.** Suppose that \(M_R = \sum_{i \in I} M_i\). Let \(m \in M_R\). Then \(m\) is called sum of elements of the submodules \(M_i\) if there exists \(m_i \in M_i\) for all \(i \in I\) such that \(m = \sum_{i \in I} m_i\).

**Definition 1.18.** (2) \(M_R\) is said to be a direct sum of the submodules \(\{M_i\}_{i \in I}\) if the additive group \((M, +)\) is a direct sum of the normal subgroups \((M_i, +), i \in I\). In this case we write \(M_R = \bigoplus_{i \in I} M_i\).

**Proposition 1.19.** (2) Suppose that \(M_R = \sum_{i \in I} M_i\). Then every element of \(M_R\) has a unique representation as a sum of elements of the submodules \(M_i\) if and only if \(M_k \cap \sum_{i \in I, i \neq k} M_i = \{0\}\) for all \(k\).

**Proposition 1.20.** (2) \(M_R = \bigoplus_{i \in I} M_i\) implies that \(M_R = \sum_{i \in I} M_i\) and \(m_i + m_j = m_j + m_i\) for all \(m_i \in M_i, m_j \in M_j\) such that \(i \neq j\).

**Lemma 1.21.** (2) Let \(M_R = \bigoplus_{i \in I} M_i\) where \(M_i\) is a submodule of \(M_R\). If \(m = \sum_{i \in I} m_i\) where \(m_i \in M_i\) and \(r \in R\) then
\[
mr = (\sum_{i \in I} m_i) r = \sum_{i \in I} (m_i r).
\]

We are now ready to define a Beidleman near-vector space.

**Definition 1.22.** (2) Let \((M_R, +)\) be a group and \(R\) a nearfield. \(M_R\) is called a Beidleman near-vector space if \(M_R\) is a nearring module which is a direct sum of irreducible submodules.

2 Description of the \(R\)-subgroups of \(R^m\)

The material presented in this section is taken from [4], in which finite dimensional Beidleman near-vector spaces were characterized as follows:

**Theorem 2.1.** (3) Let \(R\) be a (left) nearfield and \(M_R\) a (right) nearring module. \(M_R\) is a finite dimensional near-vector space if and only if \(M_R \cong R^m\) for some positive integer \(m = \dim(M_R)\).
From now on we will choose \( R \) to be a finite nearfield.

**Definition 2.2.** \((\ref{2.1})\) Let \( v_1, v_2, \ldots, v_k \) be a finite number of vectors in \( R^m \). The smallest \( R \)-subgroup of \( R^m \) containing \( v_1, v_2, \ldots, v_k \) is denoted by \( \text{gen}(v_1, \ldots, v_k) \).

Let \( LC_0(v_1, v_2, \ldots, v_k) := \{v_1, v_2, \ldots, v_k\} \) and for \( n \geq 0 \), let \( LC_{n+1} \) be the set of all linear combinations of elements in \( LC_n(v_1, v_2, \ldots, v_k) \), i.e.

\[
LC_{n+1}(v_1, v_2, \ldots, v_k) = \left\{ \sum_{w \in LC_n} w \lambda_w \mid \lambda_w \in R \, \forall \, w \in LC_n \right\}.
\]

We shall denote \( LC_n(v_1, v_2, \ldots, v_k) \) by \( LC_n \) for short when there is no ambiguity with regard to the initial set of vectors. The following theorem gives an explicit description of \( \text{gen}(v_1, \ldots, v_k) \).

**Theorem 2.3.** \((\ref{2.1})\) Let \( v_1, v_2, \ldots, v_k \in R^n \). We have

\[
\text{gen}(v_1, \ldots, v_k) = \bigcup_{i=0}^{\infty} LC_i.
\]

In order to give a description of \( \text{gen}(v_1, \ldots, v_k) \) in terms of the basis elements, the authors of \((\ref{2.1})\) first derived results analogous to those for row-reduction in vector spaces.

**Lemma 2.4.** \((\ref{2.1})\)

- For any permutation \( \sigma \) of the indices \( 1, 2, \ldots, k \), we have
  \[
  \text{gen}(v_1, \ldots, v_k) = \text{gen}(v_{\sigma(1)}, \ldots, v_{\sigma(k)}).
  \]

- If \( 0 \neq \lambda \in R \), then
  \[
  \text{gen}(v_1, \ldots, v_k) = \text{gen}(v_1 \lambda, \ldots, v_k).
  \]

- For any scalars \( \lambda_2, \lambda_3, \ldots, \lambda_k \in R \), we have
  \[
  \text{gen}(v_1, \ldots, v_k) = \text{gen}(v_1 + \sum_{i=2}^{k} \lambda_i v_i, v_2, \ldots, v_k).
  \]

- If \( w \in \text{gen}(v_1, \ldots, v_k) \) then
  \[
  \text{gen}(v_1, \ldots, v_k) = \text{gen}(w, v_1, v_2, \ldots, v_k).
  \]

**Definition 2.5.** Let \( v \in R^m \). Then \( v \) is called an \( R \)-linear combination of some finite set of vectors \( v_1, \ldots, v_k \in R^m \) if \( v \in \text{gen}(v_1, \ldots, v_k) \).

**Definition 2.6.** The \( R \)-row space of a matrix is the set of all \( R \)-linear combinations of its row vectors.
Remark 2.7.

- Let \( w \in R^m \). Note that \( w \) is a linear combination of some finite set of vectors \( v_1, \ldots, v_k \in R^m \) if \( w \in LC_1(v_1, \ldots, v_k) \). If any vector \( w \) is a linear combination of the finite set of vectors \( v_1, \ldots, v_k \in R^m \) then \( w \) is also an \( R \)-linear combination of the finite set of vectors \( v_1, \ldots, v_k \in R^m \). But the converse is not true.

- A matrix \( V \) consisting of the rows \( v_1, \ldots, v_k \in R^m \) will be denoted by \( V = \left( v_i^j \right)_{1 \leq i \leq k, 1 \leq j \leq m} \) where \( v_i^j \) is always the \( j \)-th entry of \( v_i \).

The following result gives the characterization of the \( R \)-subgroups of \( R^m \), where \( R \) is a finite nearfield. We include the proof (taken from [4]) since we will make use of the intermediate steps in the proof throughout the next section.

**Theorem 2.8.** ([4]) Let \( v_1, \ldots, v_k \) be vectors in \( R^m \). Then

\[
\text{gen}(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R,
\]

where the \( u_i \) (obtained from \( v_i \) by an explicit procedure) for \( i \in \{1, \ldots, k'\} \) are the rows of a matrix \( U = (v_i^j) \in R^{k' \times m} \) each of whose columns has at most one non-zero entry.

**Proof.** Given a set of vectors \( v_1, \ldots, v_k \in R^m \), arrange them in a matrix \( V \) whose \( i \)-th row is \( v_i \). Say \( V = \left( v_i^j \right)_{1 \leq i \leq k} \). Then \( \text{gen}(v_1, \ldots, v_k) \) is the \( R \)-row space of \( V \), which is an \( R \)-subgroup of \( R^m \). We can then do the usual Gaussian elimination on the rows. According to Lemma 2.3, the \( \text{gen} \) spanned by the rows will remain unchanged under each row operation (swapping rows, scaling rows, adding multiples of a row to another). When the algorithm terminates, we obtain a matrix \( W \in R^{k \times m} \) in reduced row-echelon form (denoted by \( RREF(V) \)). Let the non-zero rows of \( W \) be denoted by \( w_1, w_2, \ldots, w_t \) where \( t \leq k \).

Case 1: Suppose that every column has at most one non-zero entry. Then

\[
\text{gen}(v_1, \ldots, v_k) = \text{gen}(w_1, \ldots, w_t) = w_1 R + w_2 R + \cdots + w_t R,
\]

where the sum is direct. In this case we are done.

Case 2: Suppose that the \( j \)-th column is the first column that has at least 2 non-zero entries. Let \( p \) be the number of non-zero entries it has, say \( w_r^j \neq 0 = w_s^j \) with \( r < s \) are the first two non-zero entries, (we necessarily have \( r, s \leq j \)) where \( w_r^j \) is the \( j \)-th entry of row \( w_r \) and \( w_s^j \) the \( j \)-th entry of row \( w_s \). Let \( (\alpha, \beta, \gamma) \in R^3 \) such that \( (\alpha + \beta)\lambda \neq \alpha \lambda + \beta \lambda \).

We apply what we will call the “distributivity trick”:

Let \( \alpha' = (w_r^j)^{-1}\alpha \) and \( \beta' = (w_s^j)^{-1}\beta \). Then form a new row

\[
\theta = (w_r\alpha' + w_s\beta')\lambda - w_r(\alpha' \lambda) - w_s(\beta' \lambda).
\]

Since \( \theta \in LC_2(w_r, w_s) \) we have \( \theta \in \text{gen}(w_1, \ldots, w_t) \).
For $1 \leq l < j$, either $w^j_l$ or $w^j_l$ is zero because the $j$-th column is the first column that has two non-zero entries, thus $\theta^j = 0$. Note that by the choice of $\alpha, \beta, \lambda$, we have

$$\theta^j = (w^j_i \alpha + w^j_s \beta') \lambda - (w^j_i \alpha') \lambda - (w^j_s \beta') \lambda = (w^j_i (w^j_s)^{-1} \alpha + w^j_s (w^j_s)^{-1} \beta) \lambda - (w^j_i (w^j_s)^{-1} \alpha) \lambda - (w^j_s (w^j_s)^{-1} \beta) \lambda = (\alpha + \beta) \lambda - \alpha \lambda - \beta \lambda \neq 0.$$  

It follows that $\theta^j \neq 0$. Hence $\theta = (0, \ldots, 0, \theta^j, \theta^{j+1}, \ldots, \theta^n)$. We now multiply the row $\theta$ by $(\theta^j)^{-1}$, obtaining the row $\phi = (0, \ldots, 0, 1, \theta^{j+1} \phi^{-1}, \ldots, \theta^n(\theta^j)^{-1}) \in \text{gen}(w_1, \ldots, w_k)$ where $\phi^j = 1$ is the pivot that we have created.

As a next step, we form a new matrix of size $(t + 1) \times m$ by adding $\phi$ to the rows $w_1, \ldots, w_t$ (just after the row $w_s$). In this augmented matrix we replace the rows $w_r, w_s$ with $y_r = w_r - (w^j_s) \phi, y_s = w_r - (w^j_s) \phi$, respectively. This yields another new matrix composed of the rows $w_1, \ldots, w_{r-1}, y_r, \ldots, y_s, \phi, w_{s+1}, \ldots, w_t$ which has $p - 1$ non-zero entries in the $j$-th column. By Lemma 2.4, the gen of the rows of the augmented matrix is the gen of the rows of $W$ (which in turn is $\text{gen}(v_1, \ldots, v_k)$). Hence,

$$\text{gen}(v_1, \ldots, v_k) = \text{gen}(w_1, \ldots, w_r, \ldots, w_s, \ldots, w_t)$$

$$= \text{gen}(w_1, \ldots, y_r, \ldots, y_s, \phi, \ldots, w_t).$$

We keep repeating the “distributivity trick” on the $j$-th column until we form another new matrix which has only one non-zero entry at the $j$-th column.

By continuing this process, we can eliminate all columns with more than one non-zero entry. Let the final matrix have rows $u_1, u_2, \ldots, u_k$. Then

$$\text{gen}(v_1, \ldots, v_k) = \text{gen}(w_1, \ldots, w_t) = \text{gen}(u_1, \ldots, u_k^r) = u_1 R + u_2 R + \ldots + u_k^r R,$$

where the sum is direct.

\[\square\]

The procedure described in the proof of Theorem 2.8 is called the expanded Gaussian elimination (eG e algorithm). The focus of the next section is motivated by the “distributivity trick” used in the proof of Theorem 2.8.

3 On the generalized distributive set of a finite Dickson nearfield

Let $(R, +, \circ)$ be a nearfield. We use $D(R)$ to denote the set of all distributive elements of $R$, i.e.,

$$D(R) = \{ \lambda \in R : (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \text{ for all } \alpha, \beta \in R \}.$$

and $C(R)$ to denote the set of elements that commute with every element of $R$, also called the multiplicative center of $(R, \circ)$, i.e.,

$$C(R) = \{ x \in R : x \circ y = y \circ x \text{ for all } y \in R \}.$$

Theorem 3.1. \cite{10} Let $R$ be a nearfield. Then $D(R)$ under the operations of $R$ is a skewfield and is a subnearfield of $R$.  

Note that it is known in [3] that for any nearring \( R \) the multiplicative center of \( R \) is not always a subnearring of \( R \). The authors in [3] determined when \( C(R) \) is a subnearring of \( R \).

**Definition 3.2.** ([3]) Let \( R \) be a nearring and \( D(R) \) be the distributive elements of \( R \). Then the generalized center of \( R \) is the set

\[
GC(R) = \{ x \in R : x \circ y = y \circ x \text{ for all } y \in D(R) \}
\]

is called the set of elements of \( R \) that commutes with elements of \( D(R) \).

**Lemma 3.3.** ([3]) Let \( R \) be a nearfield. Then \( GC(R) \) under the operations of \( R \) is a subnearfield of \( R \).

Now consider \((R, +, \circ)\) as a finite Dickson nearfield for the Dickson pair \((q, n)\) with \( n > 1 \).

**Theorem 3.4.** ([3]) Let \( R \) be a finite Dickson nearfield that arises from the Dickson pair \((q, n)\). Then \( D(R) = C(R) \cong \mathbb{F}_q \).

So the distributive elements of a finite Dickson nearfield \( R \) under the operations of \( R \) form a subnearfield of the nearfield and under the operations of the field \( \mathbb{F}_q \) form a subfield of size \( q \). Thus there are elements \((\alpha, \beta, \lambda) \in R^3 \) such that \((\alpha + \beta) \circ \lambda \neq \alpha \circ \lambda + \beta \circ \lambda \). In the eGe algorithm described in the proof of Theorem 2.8, the “distributivity trick” requires that a triple of non-distributive elements (see equation (2)) be chosen at each step and used in the creation of new rows. This leads us to investigate the distributive elements of finite Dickson nearfields.

### 3.1 Some properties

Given \( k \in \{1, \ldots, n\} \), an \( H \)-coset shall refer to a coset of the form \( g^k H \). We have the following:

**Lemma 3.5.** Let \( R \in DN(q,n) \) where \((q,n)\) is a Dickson pair. Let \((\alpha, \beta) \in R^2 \). If \( \alpha, \beta, \alpha + \beta \) belong to the same \( H \)-coset, then \((\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \) for all \( \lambda \in R \).

**Proof.** Let \( g \) be such that \( \mathbb{F}_{q^n}^* = \langle g \rangle \) and \( H = \langle g^n \rangle \). By the finite Dickson nearfield construction, the set of all \( H \)-cosets is presented as \( \mathbb{F}_{q^n}^*/H = \{ H, g^{[1]} H, \ldots, g^{[n]} H \} \). Assume that \( \alpha, \beta, \alpha + \beta \in g^{[k]} H \) for some \( 1 \leq k \leq n \). Then

\[
(\alpha + \beta) \circ \lambda = (\alpha + \beta)\lambda^g = \alpha \lambda^g + \beta \lambda^g = \alpha \circ \lambda + \beta \circ \lambda,
\]

for all \( \lambda \in R \).

The following is an immediate consequence of Lemma 3.5.

**Corollary 3.6.** Let \( R \in DN(q,n) \) and \((\alpha, \beta) \in R^2 \) such that \( \alpha, \beta, \alpha + \beta \) belong to the same \( H \)-coset. Then \( C(D(\alpha, \beta)) = D(R) \).

Now let us look at the case for Dickson pairs \((q,n)\) where \( n = 2 \). We have the following.

**Lemma 3.7.** Let \((q,n) = (p^1,2)\) where \( p \) is prime and \( R \in DN(q,2) \). Let \((\alpha, \beta) \in R^2 \) and assume that \( \alpha, \beta, \alpha + \beta \) don’t belong all to the same \( H \)-cosets. We have \((\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \) if and only if \( \lambda \in D(R) \).
Proof. Suppose $\alpha, \beta, \alpha + \beta$ belong to different $H$-cosets which means $\alpha, \beta, \alpha + \beta$ are not all square and not all non-square. We consider the case where $\alpha + \beta \in H$ and $\alpha, \beta \in gH$ (note that the other cases are similar). If $(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda$ then we have $(\alpha + \beta)\lambda = \alpha \lambda^q + \beta \lambda^q$. Thus $\lambda^q - \lambda = 0$ and since every $\lambda \in \mathbb{F}_q$ is a solution of this equation, they are all the solutions. By Theorem 3.4 we have $\lambda \in D(R)$. The converse is straightforward.

By Lemma 3.7 we deduce the following.

**Corollary 3.8.** Let $(q, 2)$ be a Dickson pair with $q = p^l$. Let $g$ be a generator of $\mathbb{F}_{q^2}^*$ and $R$ the finite nearfield constructed with $H = \langle g^2 \rangle$. For all pairs $(\alpha, \beta) \in R^2$, $(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda$ if and only if either all $\alpha, \beta, \alpha + \beta$ belong to the same $H$-coset or $\lambda \in D(R)$.

Lemma 3.7 does not hold in general for any finite Dickson nearfield $DN_q(q, n)$ where $(q, n)$ is a Dickson pair. The following example gives an illustration.

**Example 3.9.** Let $R \in DN(q, 2)$ and $(\alpha, \beta) \in R^2$ where $\alpha, \beta, \alpha + \beta$ belong to different $H$-coset. Then by Lemma 3.7 and Corollary 3.8 $(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda$ will always lead to the equation $\lambda^q - \lambda = 0$ and all the solutions will be in $\mathbb{F}_q$. But Lemma 3.7 can fail for any positive integer $n > 2$. For instance given $R = DN_5(5, 4)$ and we take the irreducible polynomial $X^4 + 2 \in \mathbb{F}_5$ where $x$ is a root of $x^4 + 2 \in \mathbb{Z}_5[X]$. Let $g$ be such that $\mathbb{F}_{5^4}^* = \langle g \rangle$ and $H = \langle g^4 \rangle$. The quotient group is represented by

$$\mathbb{F}_{5^4}^*/H = \{gH, g^6H, g^{31}H, g^{156}H\} = \{H, gH, g^2H, g^3H\}.$$ 

Let $\alpha, \beta \in \mathbb{F}_{5^4}$, we have

$$\alpha \circ \beta = \begin{cases} \alpha \cdot \beta & \text{if } \alpha \in H \\ \alpha \cdot \beta^5 & \text{if } \alpha \in gH \\ \alpha \cdot \beta^{25} & \text{if } \alpha \in g^2H \\ \alpha \cdot \beta^{125} & \text{if } \alpha \in g^3H. \end{cases}$$

We consider $g = x + 2$. Let $\alpha = 3 \in H, \beta = x^2 + 2 \in H$. Then $\alpha + \beta \in g^2H$. In fact $\lambda = x^2 + 1 \in g^2H$ distributes over the pair $(\alpha, \beta)$. To see this, $(\alpha + \beta) \circ \lambda = (3 + x^2 + 2) \circ (x^2 + 1) = x^2 + x^4$. Also $\alpha \circ \lambda + \beta \circ \lambda = 3 \circ (x^2 + 1) + (x^2 + 2) \circ (x^2 + 1) = x^4 + x^2$. But $\lambda \notin D(R) = \mathbb{F}_5$. Note that $\lambda \notin D(R)$ but distributes over the pair $(\alpha, \beta)$. So $\lambda$ belong to a certain large distributive set of $R$.

We now introduce the following generalized distributive set for a given pair in a nearfield.

**Definition 3.10.** Let $R$ be a nearfield. Given a pair $(\alpha, \beta) \in R^2$, the generalized distributive set

$$D(\alpha, \beta) = \{\lambda \in R : (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda\}$$

is the set of elements in $R$ that distribute over the pair $(\alpha, \beta)$.

Note that in the eGe algorithm, we have to choose at every step of the creation of a new row a triple $(\alpha, \beta, \lambda) \in R^3$ such that $\lambda \notin D(\alpha, \beta)$ for the implementation of the “distributivity trick”. It is not difficult to see the following.
Lemma 3.11. Let \( R \) be a nearfield. We have
\[
\bigcap_{\alpha, \beta \in R} D(\alpha, \beta) = D(R).
\]

3.2 Some results on \( D(\alpha, \beta) \) where \( \alpha, \beta \in DN_g(q, n) \)

We remind the reader that by definition a subset \( S \subseteq \mathbb{F}_{p^n} \) that is a field is a subfield of the finite field \( \mathbb{F}_{p^n} \). Also the subfields of \( \mathbb{F}_{p^n} \) are the fields \( \mathbb{F}_{p^k} \) where \( k \) divides \( n \).

Our aim is to determine \( D(\alpha, \beta) \) where \( (\alpha, \beta) \in \mathbb{R}^2 \) for \( R \) a finite Dickson nearfield that arises from the Dickson pair \((q, n)\). Note that if \( n = 1 \) then \( DN(q, 1) \) is the set of all finite fields of order \( q \). Hence in this case \( D(\alpha, \beta) = \mathbb{F}_q \) and also \( C(D(\alpha, \beta)) = \mathbb{F}_q \).

From Lemma 3.5, Lemma 3.7 and Theorem 3.1 we deduce the following case where \( n = 2 \).

Lemma 3.12. Let \((q, 2)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and integer \( l \). Let \( g \) be a generator of \( \mathbb{F}^\ast_{q^2} \) and let \( R \) be the nearfield constructed with \( H = \langle g^2 \rangle \).

Let \((\alpha, \beta) \in \mathbb{R}^2 \). Then
(i) \( D(\alpha, \beta) \) is a subnearfield of \( R \).
(ii) \( C(D(\alpha, \beta)) \) is a subnearfield of \( R \).

Proof.
(i) Let \( R \in DN(q, 2) \) and \( \alpha, \beta \in R \). We have \( D(\alpha, \beta) = R \) or \( D(\alpha, \beta) = D(R) \). So \( D(\alpha, \beta) \) is a subnearfield of \( R \).
(ii) Suppose \( \alpha, \beta, \alpha + \beta \) belong all to the same \( H \)-coset. Then by Corollary 3.6 we have \( C(D(\alpha, \beta)) = C(R) = D(R) \) and by Theorem 3.1 \( C(D(\alpha, \beta)) \) is a subnearfield of \( R \). Furthermore, suppose \( \alpha, \beta, \alpha + \beta \) don’t belong all to the same \( H \)-coset. We have \( D(\alpha, \beta) = D(R) \). Hence by Lemma 3.3
\[
C(D(\alpha, \beta)) = C(D(R)) = D(R) \cap GC(R)
\]
is a subnearfield of \( R \).

Furthermore it is not difficult to see the following. Let \((q, n)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and integers \( l, n \). Let \( g \) be a generator of \( \mathbb{F}_{q^n}^\ast \) and let \( R \) be the nearfield constructed with \( H = \langle g^n \rangle \). Then for each positive integer \( h \) there exists a unique subfield of \( \mathbb{F}_{q^n} \) of order \( p^h \) such that \( g^{q^n - 1} \) generates its multiplicative group. In the next theorem we shall give a sufficient condition on \( \alpha, \beta \) for which \( D(\alpha, \beta) \) is a subfield of \( \mathbb{F}_{q^n} \).

Theorem 3.13. Let \((q, n)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and positive integers \( l, n \) such that \( n > 2 \). Let \( g \) be a generator of \( \mathbb{F}_{q^n}^\ast \) and \( R \) the finite nearfield constructed with \( H = \langle g^n \rangle \). Let \( \alpha, \beta \in R \). If at least two of \( \alpha, \beta, \alpha + \beta \) are in the same \( H \)-coset then \( D(\alpha, \beta) \) is a subfield of \( \mathbb{F}_{q^n} \) of order \( p^h \) for some \( h \) dividing \( l \cdot n \).

Proof.
Assume that \( \alpha, \beta, \alpha + \beta \) are all in the same \( H \)-coset. Then By Lemma 3.5 \( (\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \) for all \( \lambda \in R \). Hence \( D(\alpha, \beta) \) coincides with \( \mathbb{F}_{q^n}^\ast \).
Assume now that exactly two of $\alpha, \beta, \alpha + \beta$ are in the same $H$-coset. We consider the case where $\alpha, \beta \in g^{[s]} H$ and $\alpha + \beta \in g^{[t]} H$ for $s \neq t$ (note that the other cases are similar). Then $(\alpha + \beta) \circ \lambda = (\alpha + \beta) \lambda^q = \alpha \lambda^q + \beta \lambda^q$. Also $\alpha \circ \lambda + \beta \circ \lambda = \alpha \lambda^s + \beta \lambda^s$.

Hence

$$(\alpha + \beta) \circ \lambda = \alpha \circ \lambda + \beta \circ \lambda \Rightarrow (\alpha + \beta)(\lambda^q - \lambda^s) = 0$$

and then $\lambda = 0$ is solution of the equation. Now suppose $\lambda \neq 0$, so

$$(\alpha + \beta)(\lambda^q - \lambda^s) = 0 \Rightarrow \lambda^{q - s} - 1 = 0.$$ 

It follows that

$$\lambda^{q - s} - 1 = 0 \Rightarrow \lambda^{q - s + 1} - 1 = 0.$$ 

Continuing this procedure (raising to the power $q^s$ such that $n = s + \epsilon$) we obtain

$$\lambda^{q + s - q^s - 1} = 0.$$ 

Hence, we have $\lambda^{q - s} - 1 = 0$ where $r = t + \epsilon$ and since $\lambda^{q} = \lambda$, we get $\lambda^{q} - \lambda = 0$. We know that $q = p^l$ where $p$ is a prime number and $l, n$ are positive integers. Hence we get the following equation

$$(\Sigma) : \lambda^{p^l} - \lambda = 0 \text{ where } \lambda \in \mathbb{F}_{p^n}$$

for some positive integers $k = l \cdot r$ and $m = l \cdot n$.

(i) Suppose $k$ divides $m$. Then there exists exactly one subfield of $\mathbb{F}_{p^m}$ which is isomorphic to $\mathbb{F}_{p^k}$. So all the solutions of $(\Sigma)$ are in $\mathbb{F}_{p^m}$. Hence $D(\alpha, \beta)$ coincides with $\mathbb{F}_{p^k}$ which is a subfield of $\mathbb{F}_{p^m}$.

(ii) Suppose $k$ does not divide $m$. Note that $\lambda = 0$ is a solution of $(\Sigma)$. Set $\delta = \gcd(m, k)$. Now let $\lambda \in \mathbb{F}_{p^m}^*$ be a solution of $(\Sigma)$. So $\lambda = g^a$ for some $0 \leq a < p^m - 1$ and $g^{a(p^k - 1) - a} = 0$. Then $g^{a(p^k - 1)} = 1$. We have,

$$(p^m - 1) \text{ divides } a(p^k - 1).$$

So there exists an integer $t$ such that $a(p^k - 1) = t(p^m - 1)$. Since $\delta$ divides $m$ there exists $\theta \in \mathbb{N}$ such that $m = \delta \theta$. Also since $\delta$ divides $k$ there exists $\theta' \in \mathbb{N}$ such that $k = \delta \theta'$. So we have $p^m - 1 = (p^\delta - 1)((p^\delta)^{\theta - 1} + \ldots + p^\delta + 1)$ and $p^k - 1 = (p^\delta - 1)((p^\delta)^{\theta' - 1} + \ldots + p^\delta + 1)$. Furthermore, since

$$\gcd(p^m - 1, p^k - 1) = p^\delta - 1,$$

by Bezout’s identity there exists some integers $u$ and $v$ such that

$$u(p^m - 1) + v(p^k - 1) = p^\delta - 1.$$

Hence substituting $a(p^k - 1) = t(p^m - 1)$ we get

$$au(p^m - 1) + vt(p^m - 1) = a(p^\delta - 1).$$

Thus $(p^m - 1)$ divides $a(p^\delta - 1)$. It follows that $\frac{p^m - 1}{p^\delta - 1}$ divides $a$. So $a = \frac{p^m - 1}{p^\delta - 1}b$ where $b \in \mathbb{N}$. Now,

$$0 \leq a < p^m - 1 \Leftrightarrow 0 \leq b < p^\delta - 1.$$
Reciprocally, let \( 0 \leq b < p^\delta - 1 \) and \( \lambda_0 = g^a \). We know that \( a = \frac{p^m-1}{p^m-1} b \) and \( p^k - 1 = t'(p^\delta - 1) \) for some integer \( t' \). We have,

\[
\lambda_0^{p^k-1} - 1 = (g^a)^{t'(p^\delta-1)} - 1 = g^{(p^m-1)t'b} - 1 = 1^{t'b} - 1 = 0.
\]

It follows that \( \lambda_0 \) is a solution of the equation \( \lambda^{p^k} - \lambda = 0 \). Hence the set of solutions (denoted as \( S(\Sigma) \)) of the equation \( (\Sigma) \) for \( \lambda \in \mathbb{F}_{p^n} \) are presented as

\[
S(\Sigma) = \{0\} \cup \left\{ g \frac{p^m-1}{p^m-1} : 0 \leq b < p^\delta - 1 \right\}.
\]

The elements of \( S(\Sigma) \) are all distinct since \( g \frac{p^m-1}{p^m-1} \) is a generator of the multiplicative group of the subfield \( \mathbb{F}_{p^\delta} \) of \( \mathbb{F}_{p^n} \) (since \( \delta \) divides \( m \)). Hence

\[
|S(\Sigma)| = p^\delta - 1 + 1 = p^\delta = p^{\text{GCD}(t+n-s,n)}.
\]

So all the solutions of \( (\Sigma) \) are in the finite field of order \( p^\delta \). Hence \( D(\alpha,\beta) \) coincides with \( S(\Sigma) = \mathbb{F}_{p^\delta} \).

\[\square\]

Example 3.14. Suppose \( R = DN_q(5,4) \) with the generator \( g = x + 2 \) (see Example 3.13 regarding the construction of \( DN_q(5,4) \)). Let \( \alpha, \beta \in R \) such that \( \alpha = x + 2 \in gH \) and \( \beta = x^3 + x^2 + 2x + 3 \in g^2H \) where \( x \) is the root of the irreducible polynomial \( X^4 + 2 \in \mathbb{Z}_5[X] \). Then \( \alpha + \beta \in gH \). There exist \( \lambda_1 = x^2 + 3, \lambda_2 = 3x^2 + 2 \in D(\alpha,\beta) \) such that \( \lambda_1 \in H \) and \( \lambda_2 \in g^2H \). So the distributive elements \( \lambda_1 \) and \( \lambda_2 \) don’t belong necessarily to the same \( H \)-coset.

Note that if \( R \in DN(q,n) \) and \( (\alpha,\beta) \in R^2 \) then it is not difficult to see that \( D(R) \subseteq D(\alpha,\beta) \cap H \). Moreover we deduce the following:

Lemma 3.15. Let \( (q,n) \) be a Dickson pair with \( q = p^l \) for some prime \( p \) and integers \( l,n \). Let \( g \) be a generator of \( \mathbb{F}_{q^n}^* \) and let \( R \) be the nearfield constructed with \( H = \langle g^n \rangle \).

Let \( (\alpha,\beta,\alpha + \beta) \in g^{[r]}H \times g^{[s]}H \times H \) where \( s \neq r \) and \( r, s \) divide \( n \). Suppose that \( n \) divides \( \frac{q^s-1}{q^r-1} \) or \( n \) divides \( \frac{q^r-1}{q^s-1} \). Let \( S \) be the subset of \( \mathbb{F}_{q^n}^* \) defined by

\[
S = \left\{ g^m : q^n - 1 \text{ divides } m(q^r - 1) \text{ and } q^s - 1 \text{ divides } m(q^s - 1) \right\}.
\]

Then \( S \subseteq D(\alpha,\beta) \cap H \).

Proof. Suppose \( (\alpha,\beta,\alpha + \beta) \in g^{[r]}H \times g^{[s]}H \times H \) where \( s \neq r \) and \( r, s \) divide \( n \). Let \( \lambda \in D(\alpha,\beta) \). So \( \lambda \in \mathbb{F}_{q^n}^* \) and \( \alpha(\lambda - \lambda^q) = \beta(\lambda^{q^s} - \lambda) \). Let \( \lambda \in \mathbb{F}_{q^n}^* \), then \( \lambda = g^m \) for some \( 0 \leq m < q^n - 1 \). In fact the elements of \( S \) are solutions of \( \alpha(\lambda - \lambda^q) = \beta(\lambda^{q^s} - \lambda) \).

To see this, we have

\[
\alpha(g^m - g^{mq^r}) - \beta(g^{mq^s} - g^m) = \alpha g^m (1 - g^m(q^r-1)) - \beta g^m (1 - g^m(q^s-1)).
\]
Since $q^n - 1$ divides $m(q^r - 1)$ then there exists a positive integer $u$ such that $m(q^r - 1) = u(q^n - 1)$. Also since $q^n - 1$ divides $m(q^s - 1)$ then there exists a positive integer $v$ such that $m(q^s - 1) = v(q^n - 1)$. So we have,

$$\alpha g^m(1 - g^{m(q^r-1)}) - \beta g^m(1 - g^{m(q^s-1)}) = \alpha g^m(1 - (g^{q^n-1})^u) - \beta g^m(1 - (g^{q^n-1})^v) = \alpha g^m(1 - 1) - \beta g^m(1 - 1) = 0.$$  

So $S \subseteq D(\alpha, \beta)$. Furthermore,

$$S = \left\{ g^m : \frac{q^n - 1}{q^r - 1} \text{ divides } m \text{ and } \frac{q^n - 1}{q^s - 1} \text{ divides } m \right\} = \left\{ g^m : m = a \text{LCM}(q^n - 1, q^r - 1, q^s - 1) \text{ for } a \in \mathbb{N} \right\} = \left\{ g^a(\text{LCM}(\frac{q^n - 1}{q^r - 1}, \frac{q^n - 1}{q^s - 1})) : a \in \mathbb{N} \right\}.$$  

Since $n$ divides $\frac{q^n - 1}{q^r - 1}$ or $n$ divides $\frac{q^n - 1}{q^s - 1}$ then there exists a positive integer $b$ such that $\text{LCM}(\frac{q^n - 1}{q^r - 1}, \frac{q^n - 1}{q^s - 1}) = nb$. Thus $S = \{(g^n)^{ab} : (a, b) \in \mathbb{N}^2\} \subseteq H$.

□

We now look at $D(\alpha, \beta)$ where $\alpha, \beta, \alpha + \beta$ are all in distinct $H$-cosets. We deduce the following construction of subfield of $\mathbb{F}_{q^n}$ by making use of $D(\alpha, \beta)$.

**Theorem 3.16.** Let $(q, n)$ be a Dickson pair with $q = p^l$ for some prime $p$ and integers $l, n$ such that $n > 2$. Let $g$ be a generator of $\mathbb{F}_{q^n}$ and $R$ the finite nearfield constructed with $H = \langle g^n \rangle$. Suppose $(r, s, t) \in \mathbb{N}^3$ such that $0 < t < s < r \leq n$ where $r - s$ divides $n$ and $r - t$ divides $n$. Let $(\alpha, \beta, \alpha + \beta) \in g^{[r]}H \times g^{[s]}H \times g^{[t]}H$. Let $F_{r,s,t}(\alpha, \beta)$ be the subset of $\mathbb{F}_{q^n}$ defined by

$$F_{r,s,t}(\alpha, \beta) = D(\alpha, \beta) \cap \mathbb{F}_{q^r-s} \cap \mathbb{F}_{q^r-t}.$$  

Then $F_{r,s,t}(\alpha, \beta)$ is a subfield of $\mathbb{F}_{q^n}$.

**Proof.** Let $(\alpha, \beta, \alpha + \beta) \in g^{[r]}H \times g^{[s]}H \times g^{[t]}H$ such that $0 < t < s < r \leq n$. Let $\lambda \in D(\alpha, \beta)$, so we have $\alpha(\lambda^{q^t} - \lambda^{q^s}) = \beta(\lambda^{q^s} - \lambda^{q^t})$. Suppose $r - s$ divides $n$ and $r - t$ divides $n$. Then $\mathbb{F}_{q^r-s} \cap \mathbb{F}_{q^r-t}$ is a subfield of $\mathbb{F}_{q^n}$. Note that $\lambda \in \mathbb{F}_{q^r-s} \cap \mathbb{F}_{q^r-t} \iff \lambda^{q^{r-s}} = \lambda$ and $\lambda^{q^{r-t}} = \lambda$. It follows that $(\lambda^{q^{r-s}} - \lambda)\lambda^{q^{t-s}} = 0$ and $(\lambda^{q^{r-t}} - \lambda)\lambda^{q^{t-t}} = 0$. Thus $\lambda^{q^r} = \lambda^{q^s}$ and $\lambda^{q^r} = \lambda^{q^t}$. Also $F_{r,s,t}(\alpha, \beta) \neq \emptyset$ since $0, 1 \in F_{r,s,t}(\alpha, \beta)$. Suppose $\lambda_1, \lambda_2 \in F_{r,s,t}(\alpha, \beta)$. We have

$$\alpha((\lambda_1 + \lambda_2)\lambda^{q^r} - (\lambda_1 + \lambda_2)\lambda^{q^t}) = \alpha(\lambda_1\lambda^{q^t} + \lambda_2\lambda^{q^t} - \lambda_1\lambda^{q^t} - \lambda_2\lambda^{q^t}) = \alpha(\lambda_1^{q^t} - \lambda_2^{q^t}) + \alpha(\lambda_2^{q^t} - \lambda_2^{q^t}) = \beta(\lambda_1^{q^t} - \lambda_2^{q^t}) + \beta(\lambda_2^{q^t} - \lambda_2^{q^t}) = \beta((\lambda_1 + \lambda_2)\lambda^{q^t} - (\lambda_1 + \lambda_2)^{q^t})$$.

It follows that $\lambda_1 + \lambda_2 \in D(\alpha, \beta)$. Also $\lambda_1 + \lambda_2 \in \mathbb{F}_{q^r-s} \cap \mathbb{F}_{q^r-t}$. Hence $\lambda_1 + \lambda_2 \in \mathbb{F}_{q^n}$.
Thus

\[ \alpha((\lambda_1 \lambda_2)^{q^t} - (\lambda_1 \lambda_2)^{q^r}) = \alpha(\lambda_1^{q^t} \lambda_2^{q^t} - \lambda_1^{q^r} \lambda_2^{q^r}) = \alpha(\lambda_1^{q^t} \lambda_2^{q^t} - \lambda_1^{q^r} \lambda_2^{q^r}) = \alpha \lambda^{q^t}(\lambda_2^{q^t} - \lambda_2^{q^r}) = \lambda_1^{q^t} \beta(\lambda_2^{q^t} - \lambda_2^{q^r}) = \beta(\lambda_1^{q^t} \lambda_2^{q^t} - \lambda_1^{q^r} \lambda_2^{q^r}) = \beta(\lambda_1^{q^t} \lambda_2^{q^t} - \lambda_1^{q^r} \lambda_2^{q^r}) = \beta((\lambda_1 \lambda_2)^{q^s} - (\lambda_1 \lambda_2)^{q^t}). \]

It follows that \( \lambda_1 \lambda_2 \in D(\alpha, \beta) \). Also \( \lambda_1 \lambda_2 \in \mathbb{F}_{q^{-s}} \cap \mathbb{F}_{q^{-t}} \). Hence \( \lambda_1 \lambda_2 \in F_{r,s,t}(\alpha, \beta) \). We also have \( \lambda_1 - \lambda_2 \in F_{r,s,t}(\alpha, \beta) \). So \( (H_{r,s,t}(\alpha, \beta), +) \) is a subgroup of \( (\mathbb{F}_{q^n}, +) \).

Suppose \( \lambda \in \mathbb{F}_{q^{-s}} \cap \mathbb{F}_{q^{-t}} \). We know that if \( \lambda \in D(\alpha, \beta) \) then

\[ \alpha(\lambda^{q^t} - \lambda^{q^r}) = \beta(\lambda^{q^t} - \lambda^{q^r}) \iff \alpha(\lambda^{q^t-q^r} - 1) = -\lambda^{-q^t} \beta(\lambda^{q^s} - \lambda^{q^r}). \]

Thus

\[ \alpha(\lambda^{-q^t} - \lambda^{-q^r}) = \alpha \lambda^{-q^t}(\lambda^{q^t-q^r} - 1) = \alpha \lambda^{-q^t}(\lambda^{q^t-q^r} - 1) = -\lambda^{-q^t} \beta(\lambda^{q^s} - \lambda^{q^r}) = \beta(\lambda^{-q^s} - \lambda^{-q^r}). \]

Thus \( \lambda^{-1} \in D(\alpha, \beta) \). Hence \( \lambda_1 \lambda_2^{-1} \in F_{r,s,t}(\alpha, \beta) \). So \( (F_{r,s,t}(\alpha, \beta), \cdot) \) is a subgroup of \( (\mathbb{F}_{q^n}, \cdot) \).

**Remark 3.17.** Only the case where \( 0 < t < s < r \leq n \) is considered in the Theorem 3.16. However the other cases can be deduced in the similar way.

### 3.3 \( D(\alpha, \beta) \) presented as a vector space where \( \alpha, \beta \in DN_g(q, n) \)

In this subsection it is shown that \( D(\alpha, \beta) \) has a vector space structure. We have the following:

**Lemma 3.18.** Let \( (q, n) \) be a Dickson pair with \( q = p^l \) for some prime \( p \) and integers \( l, n \). Let \( g \) be a generator of \( \mathbb{F}_{q^n}^\times \) and \( R \) the finite nearfield constructed with \( H = \langle g^n \rangle \). Let \( (\alpha, \beta) \in R^2 \). Then \( D(\alpha, \beta) \) is an \( \mathbb{F} \)-vector space for some finite field \( \mathbb{F} \).

**Proof.** We have:

- Suppose that \( \alpha, \beta, \alpha + \beta \) are all in the same \( H \)-coset. Then \( D(\alpha, \beta) = \mathbb{F}_{q^n} \). Thus \( D(\alpha, \beta) \) is an \( \mathbb{F} \)-vector space where \( \mathbb{F} = \mathbb{F}_{q^n} \).
- Suppose that exactly two of \( \alpha, \beta, \alpha + \beta \) belong to the same \( H \)-coset. We consider the case where \( \alpha, \beta \in g^{[s]}H \) and \( \alpha + \beta \in g^{[t]}H \) for \( s \neq t \) (note that the other cases are similar). By the proof of Theorem 3.13 we have \( D(\alpha, \beta) = \mathbb{F}_{q^{\gcd(t+n-s, n)}} \). Thus \( D(\alpha, \beta) \) is an \( \mathbb{F} \)-vector space where \( \mathbb{F} = \mathbb{F}_{q^{\gcd(t+n-s, n)}} \).
Remark 3.19. It is not difficult to see that \( \phi \) is also an \( \mathbb{F}_q \)-vector space.

Lemma 3.20. Let \((q,n)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and integers \( l, n \) such that \( n > 2 \). Let \( g \) be a generator of \( \mathbb{F}_q^* \) and \( R \) the nearfield constructed with \( H = \langle g^n \rangle \). Let \((\alpha,\beta) \in R^2 \). Then there exists a positive integer \( k \) such that \( |D(\alpha,\beta)| = q^k \).

Proof. \( D(\alpha,\beta) \) is a finite dimensional vector space over \( \mathbb{F}_q \). Then \( D(\alpha,\beta) \) has a basis over \( \mathbb{F}_q \) consisting of \( k \) elements. Thus \( D(\alpha,\beta) \) has exactly \( q^k \) elements.

Our next goal is to find a basis for \( D(\alpha,\beta) \).

Computational aspect

Let \( \alpha, \beta, \alpha + \beta \in DN_q(q,n) \) such that \( \alpha \in g^{[r]q}H \), \( \beta \in g^{[s]q}H \) and \( \alpha + \beta \in g^{[t]q}H \) where \( r, s \) and \( t \) are all different. We have

\[
(\alpha + \beta) \circ \lambda = \alpha \circ \lambda \circ \beta \circ \lambda \iff \alpha(\lambda^{q^t} - \lambda^{q^r}) = \beta(\lambda^{q^r} - \lambda^{q^t})
\]

for all \( \lambda \in \mathbb{F}_{q^n} \). We resort to computational methods in order to check the nature of the distributive elements \( D(\alpha,\beta) \). We derive an algorithm called "DSS" (Distributive Set Subfields) which tests whether \( D(\alpha,\beta) \) is a finite field.

We construct a function \( \phi \) from \( \mathbb{F}_{q^n} \) to itself that maps \( \lambda \) to \( \alpha(\lambda^{q^t} - \lambda^{q^r}) - \beta(\lambda^{q^r} - \lambda^{q^t}) \). This function will be zero if and only if \( \lambda \) is a solution to the equation \( \alpha(\lambda^{q^t} - \lambda^{q^r}) = \beta(\lambda^{q^r} - \lambda^{q^t}) \). Moreover, \( \phi \) is an \( \mathbb{F}_q \)-linear map, so it suffices to compute it on a basis. A basis of \( \mathbb{F}_{q^n} \) is \( \{1,g,g^2,\ldots,g^{n-1}\} \). The function \( \phi \) is entirely determined by the vectors \( \phi(1), \phi(g), \ldots, \phi(g^{n-1}) \). We can represent each vector \( \phi(g^j) \) for \( 0 \leq j \leq n-1 \) as

\[
\phi(g^j) = m^j_1 + m^j_2 g + \ldots + m^j_{(n-1)} g^{n-1}
\]

where \( m^j_1 \in \mathbb{F}_q \) with \( 0 \leq i \leq n-1 \). Thus \( \phi \) is entirely determined by the values of the matrix of size \( n \times n \) defined by \( M = (m^j_i)_{0 \leq i \leq n-1} \). Let \( \lambda \in \mathbb{F}_{q^n} \), there exist \( \lambda_0, \ldots, \lambda_{n-1} \in \mathbb{F}_q \) such that \( \lambda =
Example 3.21. Suppose that $(q,n) = (4,3)$. Let $g$ be such that $\mathbb{F}_4^* = \langle g \rangle$ and $H = \langle g^3 \rangle$. We know that by Theorem 2.13 if at least two of $\alpha, \beta, \alpha + \beta$ belong to the same $H$-coset then $D(\alpha, \beta)$ is a subfield of $\mathbb{F}_q^n$. Furthermore for all $\alpha \in H, \beta \in gH$ and $(\alpha + \beta) \in g^2H$, $D(\alpha, \beta)$ is a finite field.

1. Suppose that $(q,n) = (4,3)$. Let $g$ be such that $\mathbb{F}_4^* = \langle g \rangle$ and $H = \langle g^3 \rangle$. We know that by Theorem 3.13, if at least two of $\alpha, \beta, \alpha + \beta$ belong to the same $H$-coset then $D(\alpha, \beta)$ is a subfield of $\mathbb{F}_q^n$. Furthermore for all $\alpha \in H, \beta \in gH$ and $(\alpha + \beta) \in g^2H$, $D(\alpha, \beta)$ is a finite field.

2. Suppose that $(q,n) = (5,4)$. Then $D(\alpha, \beta)$ is also a finite field for every $\alpha, \beta \in D\mathcal{N}_q(5,4)$ where $\mathbb{F}_{5^4}^* = \langle g \rangle$ and $H = \langle g^4 \rangle$.

3. Suppose that $(q,n) = (7,9)$. Let $g$ be such that $\mathbb{F}_7^* = \langle g \rangle$ and $H = \langle g^9 \rangle$. We know that $D(\alpha, \beta)$ is an $\mathbb{F}_7$-vector space. Also $\mathbb{F}_{7^9}^*$ is an $\mathbb{F}_7$-vector space with a basis $\{1, g^2, \ldots, g^8\}$. We take some elements

$$\alpha = 4g^8 + 5g^7 + 3g^4 + 6g^3 + 6g^2 + 6g + 4 \in \mathbb{F}_{7^9}^*$$

$$\beta = 5g^8 + 3g^7 + g^6 + 3g^5 + 3g^4 + g^3 + 3g^2 + 6g + 6 \in \mathbb{F}_{7^9}^*$$

such that $\alpha, \beta, \alpha + \beta$ are in distinct $H$-cosets. Then it turns out that a basis of $D(\alpha, \beta)$ is $\{1, g + 2g^2 + 6g^3 + 6g^6 + 5g^7 + 6g^8\}$ and has dimension 2. Then

$$D(\alpha, \beta) = \left\{ \sum_{i=1}^{2} v_i \alpha_i \mid \alpha_i \in \mathbb{F}_7 \right\}$$

where $v_1 = 1$ and $v_2 = g + 2g^2 + 6g^3 + 6g^6 + 5g^7 + 6g^8$. Hence $|D(\alpha, \beta)| = 7^2$ and 2 does not divide 9. Thus $D(\alpha, \beta)$ is not a finite field.

4. We also consider the Dickson pair $(q,n) = (5,8)$. Let $g$ be such that $\mathbb{F}_{5^8}^* = \langle g \rangle$ and $H = \langle g^8 \rangle$. We know that $D(\alpha, \beta)$ is an $\mathbb{F}_5$-vector space. Also $\mathbb{F}_{5^8}^*$ is an $\mathbb{F}_5$-vector space with a basis $\{1, g^2, \ldots, g^7\}$. We take a pair of elements in $\mathbb{F}_{5^8}^*$

$$\alpha = 3g^6 + 4g^4 + 3g^3 + 3g^2 + 2g + 2$$

$$\beta = 4g^7 + g^6 + g^5 + 3g^4 + 4g^2 + 3g + 2$$

such that $\alpha, \beta, \alpha + \beta$ are in distinct $H$-cosets. Then

$$D(\alpha, \beta) = \left\{ \sum_{i=1}^{2} v_i \alpha_i \mid \alpha_i \in \mathbb{F}_5 \right\}$$
where \( v_1 = 1 \) and \( v_2 = 2g^7 + 3g^6 + g \) and \( D(\alpha, \beta) \) has dimension 2. Hence \(|D(\alpha, \beta)| = 5^2\). Note that 2 divides 8. But \( D(\alpha, \beta) \) is not closed under the finite field multiplication. To see this,
\[
v_2^2 = v_2 \cdot v_2 = 4g^7 + g^6 + 2g^5 + g^4 + 2g^3 + 3g^2 + 2g + 4.
\]

In fact
\[
v_2^2 \notin D(\alpha, \beta).
\]

Hence \( D(\alpha, \beta) \) is not a finite field.

The Example 3.21 leads us to deduce that if \( \alpha, \beta, \alpha + \beta \) belong to distinct \( H\)-cosets then \( D(\alpha, \beta) \) is not in general a subfield of the finite field \( \mathbb{F}_q^n\).

During 1971 and 1972, Dancs showed in \([8, 9]\) that the subnearfield structure of a finite nearfield is analogous to the subfield structure of finite fields.

**Theorem 3.22.** \((8, 9)\) Let \( R \) be a finite nearfield of order \( q^n \), where \( q = p^l \) for some prime \( p \).

(i) If \( K \) is a subnearfield of \( R \), then \( |K| = p^h \) with \( h \) dividing \( l \cdot n \).

(ii) Conversely, if \( h \) divides \( l \cdot n \), then \( R \) has a unique subnearfield \( K \) of order \( p^h \).

Let \( R \in DN(q, n) \) where \( n > 2 \). Let \( (\alpha, \beta) \in R^2 \). Looking at \( D(\alpha, \beta) \) where \( \alpha, \beta, \alpha + \beta \) are all in distinct \( H\)-cosets, assume that \( (\alpha, \beta, \alpha + \beta) \in g^{[r]_g}H \times g^{[s]_g}H \times g^{[t]_g}H \) such that \( r, s, t \) are all distinct. Then
\[
D(\alpha, \beta) = \{ \lambda \in R : \alpha(\lambda^q - \lambda^q) = \beta(\lambda^q - \lambda^q) \}.
\]

By Example 3.21 and appealing to Theorem 3.22 if we take the Dickson pair \((7, 9)\) we see that there exist some pairs \((\alpha, \beta)\) such that \( D(\alpha, \beta) \) is not a subnearfield of \( DN_q(7, 9) \).

Furthermore by proof of Theorem 3.13 the following is an immediate consequence:

**Corollary 3.23.** Let \((q, n)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and positive integers \( l, n \) such that \( n > 2 \). Let \( g \) be a generator of \( \mathbb{F}_q^* \) and let \( R \) be the nearfield constructed with \( H = \langle g^n \rangle \). Let \( (\alpha, \beta) \in R^2 \). We have the following:

(i) If all \( \alpha, \beta, \alpha + \beta \) belong to the same \( H\)-coset then \( D(\alpha, \beta) = R \) and so is also a subnearfield of \( R \).

(ii) If two of \( \alpha, \beta, \alpha + \beta \) belong to \( g^{[s]_g}H \) and the third to \( g^{[t]_g}H \) such that \( \gcd(t + n - s, n) = 1 \) where \( s \neq t \) then by Theorem 3.13 \( D(\alpha, \beta) \) is a subnearfield of \( R \).

Furthermore \( C(D(\alpha, \beta)) = C(D(R)) = D(R) \cap GC(R) \).

**Remark 3.24.** Let \((q = p^l, n)\) be a Dickson pair and \( R = DN_g(q, n) \) where \( g \) is a generator of \( \mathbb{F}_q^* \) and \( R \) the finite nearfield constructed with \( H = \langle g^n \rangle \). Every \( \mathbb{F}_{p^k} \) with \( k \) dividing \( l \) is a subnearfield of \( DN_g(q, n) \). To see this, by Theorem 3.13 \( D(R) \) is a subnearfield of \( R \). Also by Theorem 3.13 \( D(R) \) is a finite field, so isomorphic to \( \mathbb{F}_{p^k} \). It is known that \( \mathbb{F}_{p^k} \) can be embedded into \( \mathbb{F}_{p^l} \) if and only if \( k \) divides \( l \). So every \( \mathbb{F}_{p^k} \) with \( k \) dividing \( l \) can be embedded into \( DN_g(q, n) \). Note that they have different multiplication, but \( \mathbb{F}_{p^k} \) is isomorphic to a subfield of \( \mathbb{F}_{p^l} \) which is a subnearfield of \( DN_g(q, n) \). Hence \( \mathbb{F}_{p^k} \) is a subnearfield of \( DN_g(q, n) \). Observe that \( k \) must divide \( l \),
Remark 4.5. Let $\gen w$ in each column. We have, $\gen k$.

Definition 4.4. Suppose $\gcd(t + n - s, n) \neq 1$ then $l \cdot \gcd(t + n - s, n)$ can not divide $l$. Hence $D(\alpha, \beta)$ can not be a subnearfield of $D(R) = F_{p^j}$.

4 Further results on $R$-subgroups

Let $R$ be a finite nearfield. All the results in this section make use of Theorem 2.8 where at each “distributivity trick”, a triple $(\alpha, \beta, \lambda) \in R^3$ such that $\lambda \notin D(\alpha, \beta)$ is chosen within an application of the eGe algorithm.

4.1 Some properties

In this subsection, we study the notion of $R$-dimension and $R$-basis of $R$-subgroups.

Definition 4.1. A finite set $V = \{v_1, \ldots, v_k\}$ of non-zero vectors in $R^n$ is $R$-linearly dependent if there exists $v_i \in V$ such that $v_i \in \gen(v_1, \ldots, v_i, \ldots, v_k)$.

Note that we use $\{v_1, \ldots, v_i, \ldots, v_k\}$ to denote the fact that the vector $v_i$ has been removed from the set of vectors $\{v_1, \ldots, v_k\}$.

Lemma 4.2. Let $R$ be a finite nearfield and $v_1, \ldots, v_k \in R^m$. Then $|\gen(v_1, \ldots, v_k)| = |R|^{k'}$ where $k'$ is the number of non-zero rows obtained after performing the eGe algorithm on the vectors $v_1, \ldots, v_k$.

Proof. By Theorem 2.8, we have $\gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} u_i R$ where $U = (u_i^j) \in R^{k' \times m}$ is the final matrix after the expanded Gaussian elimination with the property that all its columns have at most one non-zero entry. Hence $|\gen(v_1, \ldots, v_k)| = |\bigoplus_{i=1}^{k'} u_i R| = |u_1 R| \times |u_2 R| \times \cdots \times |u_{k'} R| = |R|^{k'}$. \hfill $\square$

In particular, we obtain:

Corollary 4.3. Let $R$ be a finite nearfield and $T$ an $R$-subgroup of $R^m$. Then $|T| = |R|^k$ for some $k \leq m$.

In analogy to the notion of a basis of a subspace in the theory of vector spaces, we introduce what we will call $R$-basis and $R$-dimension of an $R$-subgroup of the finite dimensional Beidleman near-vector spaces $R^m$.

Definition 4.4. Let $R$ be a finite nearfield and $T$ an $R$-subgroup of $R^m$. There exist some vectors $v_1, \ldots, v_k \in R^m$ such that $\gen(v_1, \ldots, v_k) = T$. By the eGe algorithm, the finite set of non-zero row vectors $\{u_1, \ldots, u_{k'}\}$ obtained will be called an $R$-basis of $T$ and the number $k'$ will be called the $R$-dimension of $T$.

Remark 4.5. Let $R$ be a finite nearfield. Suppose there exist $v_1, \ldots, v_k \in R^m$ and $w_1, \ldots, w_l \in R^m$ such that $\gen(v_1, \ldots, v_k) = \gen(w_1, \ldots, w_l) = T$. By Theorem 2.8 we have $\gen(v_1, \ldots, v_k) = \bigoplus_{i=1}^{k'} \mu_i R$ and $\gen(w_1, \ldots, w_l) = \bigoplus_{i=1}^{l'} \nu_i R$ such that $(\mu_i^j)_{1 \leq i \leq k'}$ and $(\nu_i^j)_{1 \leq i \leq l'}$ are some matrices that have at most one non-zero entry in each column. We have, $|\gen(v_1, \ldots, v_k)| = |\gen(w_1, \ldots, w_l)|$. Then $|R|^{k'} = |R|^{l'}$. Thus $k' = l'$. Thus the $R$-dimension of $T$ is well-defined.
Definition 4.6. Let $R$ be a finite nearfield and $T$ an $R$-subgroup of $R^m$. $V$ generates $T$ if $V \subseteq T$ and $\text{gen}(V) = T$.

Definition 4.7. Let $R$ be a finite nearfield and $T$ a $R$-subgroup of $R^m$. $V$ is a seed set for $T$ if $V$ is $R$-linearly independent and $V$ generates $T$.

Definition 4.8. Let $R$ be a finite nearfield and $T$ an $R$-subgroup of $R^m$. The seed number of $T$ is the minimal cardinality of all the seed sets, i.e., $s(T) = \min_{V \in \mathcal{B}} |V|$ where $\mathcal{B}$ is the set of seed sets for $T$.

Remark 4.9. Let $R$ be a finite nearfield and $T$ an $R$-subgroup of $R^m$. Then the seed number $s(T)$ is well-defined. Note that for every $R$-subgroup $T$, $\text{gen}(T) = T$ (i.e., $T$ is generated by all its elements), then $s(T) \leq |T|$. Thus $s(T)$ is well-defined.

Lemma 4.10. Let $R$ be a finite nearfield and $T$ an $R$-subgroup of $R^m$. Then

$$R \cdot \text{dim}(T) = \max_{V \in \mathcal{B}} |V|$$

where $\mathcal{B}$ is the set of seed sets for $T$.

Proof. Let $T$ be an $R$-subgroup of $R^m$. Suppose $V$ is a seed set for $T$ containing $k$ vectors. Then $\text{gen}(V) = T$. By the eGe algorithm we have $\text{gen}(V) = \bigoplus_{i=1}^{k} u_i R$ where $(u_i^j)_{1 \leq j \leq k'}$ is a matrix that has at most one non-zero entry in each column. Since $V$ is $R$-linearly independent, $k' \geq k$. Thus $R \cdot \text{dim}(T) \geq |V|$. $\square$

Example 4.11. Let us consider the finite dimensional Beidleman near-vector space $(R^m, R)$ where $R$ is a finite nearfield. Suppose $m = 1$. Then $s(R) = 1$. Suppose $n = 2$. Since $\text{gen}(v) = vR$ for all $v \in R^2$, we have $s(R^2) \neq 1$. Thus $s(R^2) = 2$. Suppose $m = 3$. Let $v_1 = (1,1,0)$ and $v_2 = (0,1,1)$ in $R^3$ such that $\text{gen}(v_1, v_2) = \text{gen}(e_1, e_2, e_3) = R^3$ where $e_1 = (1,0,0), e_2 = (0,1,0)$ and $e_3 = (0,0,1)$. So $\{e_1, e_2, e_3\}$ and $\{v_1, v_2\}$ are some seed sets for $R^3$. A seed set of maximum size is $\{e_1, e_2, e_3\}$ and a seed set of minimum size is $\{v_1, v_2\}$. Thus $s(R^3) = 2$ and $R \cdot \text{dim}(R^3) = 3$.

Lemma 4.12. Let $R$ be a finite nearfield and $V$ a finite set of vectors in $R^m$. If $\text{gen}(V) = T$, then $V$ contains a seed set for $T$.

Proof. Let $V = \{v_1, \ldots, v_k\}$ such that $\text{gen}(V) = T$. Using Lemma 2.4, keep removing elements from $V$ that do not contribute to $\text{gen}(V)$ until we find a seed set for $T$. Note that the order in which we remove elements matters, in the sense that the seed sets we get at the end may have different sizes. $\square$

Lemma 4.13. Let $R$ be a finite nearfield and $V$ a finite set of vectors in $R^m$ such that $\text{gen}(V) = T$. Assume that the vectors in $V$ are arranged in a matrix $M$ of size $k \times m$. Then $s(T)$ is less than or equal to the number of pivots that we get in the reduced row echelon form of $M$.

Proof. Let $V$ be a seed set for $T$. Suppose $V$ contains the vectors $v_1, \ldots, v_k \in R^m$ arranged in a matrix $M \in R^{k \times m}$. The reduced row echelon form of $M$ gives another matrix $M' \in R^{t \times m}$ whose set of non-zero row vectors is $W = \{w_1, \ldots, w_t\}$ where $t \leq k$. By Lemma 2.4 we have $T = \text{gen}(V) = \text{gen}(W)$ and $W$ is $R$-linearly independent. So $W$ is also a seed set for $T$. If $W$ is minimum sized then $s(T)$ is the number of elements in $W$ which correspond to the number of pivots of $M' = \text{RREF}(M)$. Else $s(T)$ is less than the number of elements in $W$. $\square$
4.2 Seed number of $R^m$

Let $R$ be a nearfield and $T$ an $R$-subgroup of $R^m$ where $m$ is a positive integer. By definition $s(T)$ is the minimum size of all seed sets of $T$. In the theory of vector spaces, the dimension of a subspace is at most the dimension of the entire space. Similarly, the $R$-dimension of an $R$-subgroup of $R^m$ is at most the $R$-dimension of the entire space. Thus $s(T) \leq R\text{-dim}(T) \leq m$.

In analogy to the theory of vector spaces we have the following.

**Lemma 4.14.** Let $v = (v_i)_{1 \leq i \leq m}, w = (w_i)_{1 \leq i \leq m} \in R^m$. Suppose there exists $(v_j, w_j) = \rho(v_i, w_i)$ where $i \neq j$ and $\rho \in R$. Then by elimination of one of the pairs $(v_i, w_i)$ or $(v_j, w_j)$ from $v$ and $w$, we obtain the new vectors $v' = (v_1, \ldots, \hat{v}_i, \ldots, v_m) \in R^{m-1}, w' = (w_1, \ldots, \hat{w}_i, \ldots, w_m) \in R^{m-1}$ or $v' = (v_1, \ldots, \hat{v}_j, \ldots, v_m) \in R^{m-1}, w' = (w_1, \ldots, \hat{w}_j, \ldots, w_m) \in R^{m-1}$ with

$$R\text{-dim}\left(\text{gen}(v, w)\right) = R\text{-dim}\left(\text{gen}(v', w')\right).$$

**Proof.** Let $v = (v_i)_{1 \leq i \leq m}, w = (w_i)_{1 \leq i \leq m} \in R^m$ arranged in a matrix

$$V = \begin{bmatrix} v_1 & v_2 & v_3 & \ldots & v_m \\ v_1 & v_2 & v_3 & \ldots & v_m \end{bmatrix} \in R^{2 \times m}.$$ Suppose for simplicity that $(v_2, w_2) = \rho(v_1, w_1) = (\rho v_1, \rho w_1)$ where $v_1, v_2, w_1, w_2, \rho \in R$. We apply the eGe algorithm on the set $\{v, w\}$. Note that eliminating the non-zero entries in the first column of $V$ will also automatically eliminate the non-zero entries in the second column of $V$. Hence, the number of additional rows created as we apply eGe algorithm on $\{v, w\}$ is the same as the number of additional rows we will create when we apply the eGe on $\{v', w'\}$ where $v' = (v_2, \ldots, v_m) \in R^{m-1}, w' = (w_2, \ldots, w_m) \in R^{m-1}$. \hfill \Box

We now deduce the following:

**Theorem 4.15.** Let $R$ be a finite Dickson nearfield that arises from the Dickson pair $(q, n)$ and $T$ be an $R$-subgroup of $R^m$. If $s(T) = 2$, then

$$2 \leq R\text{-dim}(T) \leq q^n + 1.$$  

**Proof.** Suppose $T$ is an $R$-subgroup of $R^m$ and $s(T) = 2$. Then there exist minimal generators of $T$ denoted as $v_1 = (v_1^1, \ldots, v_1^m), v_2 = (v_2^1, \ldots, v_2^m)$, i.e., $\text{gen}(v_1, v_2) = T$ where $v_1$ and $v_2$ are arranged in a matrix $V \in R^{2 \times m}$.

Consider the pairs $(v_1^i, v_2^j)$ with $v_1^i \neq 0 \neq v_2^j$ where $1 \leq i \leq m$. Assume there are two such pairs such that

$$v_1^i = \rho v_1^1, \quad v_2^j = \rho v_2^1 \quad \text{for } i \neq j \quad \text{and } \rho \in R. \quad (3)$$

Note that we may think of $(v_1^i, v_2^j)$ as a multiple of $(v_1^1, v_2^1)$. For simplicity, let $i = 1, j = 2$. Thus we can write $v_1^2 = \rho v_1^1$ and $v_2^2 = \rho v_2^1$.

Now the expanded Gaussian elimination algorithm (in the proof of Theorem 2.8) returns a seed set $\{u_1, \ldots, u_k\}$ (where $k = R\text{-dim}(T)$) for $T$ such that every column
of the matrix with rows \(u_1, \ldots, u_k\) has at most one non-zero entry. In this process, we take \(R\)-linear combinations of the rows to form new rows, e.g., suppose we have \(\alpha, \beta, \lambda \in R\) and we consider the vector \(z_1 = (v_1 \alpha + v_2 \beta) \lambda\). So \(z_1 \in LC_2(v_1, v_2)\). Then
\[
z_1^2 = (v_1^2 \alpha + v_2^2 \beta) \lambda = (\rho v_1^2 \alpha + \rho v_2^2 \beta) \lambda = \rho (v_1^2 \alpha + v_2^2 \beta) \lambda = \rho z_1.
\]

Thus every vector created in this manner satisfies \(z_1^2 = \rho z_1\). In fact for \(z_1 \in LC_m(v_1, v_2)\) where \(m\) is a positive integer, we will still have that \(z_1^2 = \rho z_1\). At the end of the expanded Gaussian elimination, \(u_1\) is an \(R\)-linear combination of \(v_1\) and \(v_2\), so we will have \(u_1 = 1, u_2 = \rho\) where the column is indicated by the super-script.

Furthermore, if \(v_1^i = 0\) or \(v_2^i = 0\) then the pair \((v_i^1, v_i^2) = (0, v_2^i) = v_2^i(0, 1)\) or \((v_i^1, v_i^2) = (v_1^i, 0) = v_1^i(1, 0)\). Else \(v_1^i \neq 0 \neq v_2^i\) then \((v_i^1, v_i^2) = v_i^1(1, (v_i^1)^{-1}v_2^i) = v_i^1(1, r)\) where \(r = (v_i^1)^{-1}v_2^i\). So we can write any pair as a multiple of one of the following pairs: \((1, 0), (0, 1)\) or \((1, r)\) for \(r \in R^*\) (which can’t be expressed as multiples of other pairs in \(R^2\)). For example, suppose \((\rho_1, 0) = \rho_1(1, 0), (0, \rho_3) = \rho_3(0, 1)\) and \((\rho_2, \rho_4) = \rho_2(1, r)\) where \(r = \rho_2^{-1}\rho_4, \rho_1, \rho_2, \rho_3, \rho_4 \in R^*\). Then
\[
R\text{-dim}\ (gen((\rho_1, 0, \rho_2), (0, \rho_3, \rho_4))) = R\text{-dim}\ (gen((1, 0, 1), (0, 1, r))).
\]

By Lemma [14.14] for any two pairs \((v_i^1, v_i^2)\) and \((v_j^1, v_j^2)\) for \(i \neq j\) satisfying the above condition [3], we may eliminate one of them without changing the \(R\)-dimension of the \(R\)-subgroup generated by \(v_1, v_2\). Hence the \(R\)-dimension of \(T\) cannot exceed the maximal number of pairs where we can not eliminate any other pairs of the form \((1, 0), (0, 1)\) or \((1, r)\) for \(r \in R^*\). Thus
\[
\max_{v_1, v_2 \in R^m} \{ R\text{-dim}\ (gen(v_1, v_2)) \} = 2 + (|R| - 1) = 1 + |R| = q^n + 1.
\]

\[\square\]

**Remark 4.16.** Let \(T\) be an \(R\)-subgroup of \(R^m\) for a positive integer \(m\). Assume that \(s(T) = 2\). By Theorem [4.15] the \(R\)-dimension of \(T\) is restricted to a specific range such that \(s(T) \leq R\text{-dim}(T) \leq |R| + 1\).

**Example 4.17.** As in [13], p.257), let us consider the finite field \((\mathbb{F}_{3^2}, +, \cdot)\) with
\[
\mathbb{F}_{3^2} := \{0, 1, 2, x, 1 + x, 2 + x, 2x, 1 + 2x, 2 + 2x\},
\]
where \(x\) is a zero of \(X^2 + 1 \in \mathbb{Z}_3[X]\) with the new multiplication defined as
\[
a \circ b := \begin{cases} a \cdot b & \text{if } a \text{ is a square in } (\mathbb{F}_{3^2}, +, \cdot) \\ a \cdot b^3 & \text{otherwise} \end{cases}
\]
This gives the smallest finite Dickson nearfield \(R = DN_o(3, 2)\) which is not a field (here \(\mathbb{F}_{3^2}^* = \langle y \rangle\) and \(H = \langle y^2 \rangle\)). Let \(v = (x + 2, x + 1, 1, 1, 2x + 1, x + 1, 2, 0, 2x + 1, 2x + 2, x + 2, 2x + 1, 2x + 1, x + 2, 2x + 1, x + 1, 2x + 2, x + 2, x + 2, x + 1)\) and \(w = (2x, 2, 1, 2x + 2, 0, 2r, 2, 2x + 1, x + 1, 0, 2x + 1, 1, x + 1, 2x + 2, 2x + 2, 2x + 2, x + 1) \in R^{19}\).

Then \(T = gen(v, w)\) is an \(R\)-subgroup of \(R^{19}\) and we have \(R\text{-dim}(T) = 10\).

**Remark 4.18.** In contrast to the theory of vector spaces, the following does not always hold: \(R\text{-dim}\ (gen(v_1, \ldots, v_k)) = R\text{-dim}\ (gen(w_1, \ldots, w_m))\) where a matrix \(V \in R^{k \times m}\) contains the rows \(v_1, \ldots, v_k\) and the columns \(w_1, \ldots, w_m\). To see this, suppose
Let \( R \in DN(3,2) \) (from Example 4.14). Let \( v_1 = (1,2,x,0,0), v_2 = (0,0,0,1,0), v_3 = (1,0,0,0,1) \) and \( w_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 2 \\ 0 \end{bmatrix}, w_2 = \begin{bmatrix} x \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, w_3 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, w_4 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, w_5 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \). In fact \( R \)-dim \((\text{gen}(v_1, v_2, v_3)) = 4 \) but \( R \)-dim \((\text{gen}(w_1, w_2, w_3, w_4, w_5)) = 3. \)

In the next theorem we shall determine the seed number of the finite dimensional Beidleman near-vector space \( R^m \) where \( R \) is a finite Dickson nearfield. This is accomplished by finding two vectors \( v, w \in R^m \) such that \( \text{gen}(v, w) = R^m \) for some positive integer \( m \) such that \( m \leq |R| + 1 \). The result is the converse of Theorem 4.15.

**Theorem 4.19.** Let \( R \) be a finite Dickson nearfield that arises from the Dickson pair \((q,n)\). For every value \( m \) satisfying \( 2 \leq m \leq q^n + 1 \), we have \( s(R^m) = 2. \)

**Proof.** For \( 2 \leq m \leq |R| + 1 \), we choose \( v = (1,0,1,\ldots,1) \) and \( w = (0,1, w^3, \ldots, w^m) \in R^m \) arranged in a matrix

\[
V = \begin{bmatrix}
1 & 0 & 0 & \cdots & 1 \\
0 & 1 & w^3 & \cdots & w^m
\end{bmatrix} \in R^{2 \times m},
\]

where each element \( w^j \neq 1 \) for \( j \in \{3, \ldots, m\} \) is a non-zero distinct element (i.e, \( w^j \in R^* \setminus \{1\} \)). Note that all the pairs

\[
(1,0), (0,1), (1,w^3), \ldots, (1,w^j), \ldots, (1,w^m)
\]

satisfy the following condition

\[
(v_j, w_j) \neq \alpha(v_i, w_i) \text{ for all } i, j \text{ where } i \neq j \text{ and } \alpha \in R^*.
\]

Thus by implementing the eGe algorithm (the explicit procedure in the proof of Theorem 4.18) on the initial matrix \( V \), we create at least \( m - 2 \) additional rows (since the first two columns each have exactly one non-zero entry). Hence we may apply the “distributivity trick” on the third column and so on. Note that the process will stop after creating exactly \( m - 2 \) new rows so that at the end of eGe, we will get in total \( m \) rows so that \( \text{gen}(v, w) = \bigoplus_{i=1}^{m} e_i R = R^m \) where \( \{e_i\}_{i=1, \ldots, m} \) is the standard basis. Thus \( s(R^m) = 2. \)

**Example 4.20.** Let \( R \in DN(3,2) \). There exist \( v = (1,2x+2,x,0,x) \) and \( w = (2,2x,1,2,x) \in R^5 \) such that \( \text{gen}(v, w) = R^5 \). Thus \( s(R^5) = 2. \)

We have seen that it takes two vectors that belong to \( R^m \) under the condition that \( m \leq |R| + 1 \) to generate the whole space.

5 Concluding comments

Let \( R \) be a finite Dickson nearfield that arises from the Dickson pair \((q,n)\). We have determined \( D(\alpha, \beta) \) for a given \((\alpha, \beta) \in R^2 \) and showed that it is used in the determination of \( s(R^m) \) by the implementation of the eGe algorithm. Some computational methods have been implemented in Sage. Note that the proof of Theorem 4.18 taken from [1] was included to illustrate to the readers the eGe algorithm and
the motivation of the generalised distributive set. In contrast to the situation for \( D(R) \) by the work of Zemmer in [16] (see Theorem 3.1) we found that \( D(\alpha, \beta) \) is not always a subnearfield of \( R \). It shouldn’t be too hard to use the characterization of the 7 exceptional finite nearfields to determine their generalized distributive sets. Furthermore if \( n > 2 \) and \( \alpha, \beta, \alpha + \beta \) belong all to distinct \( H \)-cosets then the multiplicative center of \( D(\alpha, \beta) \) can’t be characterized since \( D(\alpha, \beta) \) is not always a multiplicative subgroup of \( R \). It seems appropriate to close with further problems on the generalized distributive set and seed number.

- Let \((q, n)\) be a Dickson pair with \( q = p^l \) for some prime \( p \) and integers \( l, n \) such that \( n > 2 \). Let \( g \) be a generator of \( \mathbb{F}_{q^n}^* \) and \( R \) the nearfield constructed with \( H = \langle g^n \rangle \). Let \((\alpha, \beta, \alpha + \beta) \in g^{\frac{q^r-1}{q-1}} H \times g^{\frac{q^s-1}{q-1}} H \times g^{\frac{q^t-1}{q-1}} H \) such that \( r, s, t \) are all distinct. Can we find a condition on \((q, n)\) such that \( D(\alpha, \beta) \) is always a subfield of \( \mathbb{F}_{q^n} \)?
- Can we find a necessary and sufficient condition on the Dickson pair \((q, n)\) such that \( D(\alpha, \beta) \) is always a subnearfield of \( DN_g(q, n) \)?
- Let \( T \) be an \( R \)-subgroup of \( R^m \). In the general setting if \( s(T) = k \) what are the possible \( R \)-dimensions for \( T \)?

6 Acknowledgments

I thank Dr Gareth Boxall and Dr Karin-Therese Howell for their advice on this work. I thank as well Georg Anegg for his collaborations. I worked on this paper while studying toward my PhD at Stellenbosch University.

7 Funding

I am grateful for funding by AIMS (South Africa) and DAAD. This work is based on the research supported in part by the National Research Foundation of South Africa (Grant Numbers 93050, 96234).

8 Appendix

Let \( R \) be a finite Dickson nearfield that arises from the Dickson pair \((q, n)\). In this section we give more details about the pseudo-code that we have implemented in Sage for some tests on \( D(\alpha, \beta) \) for a given \((\alpha, \beta) \in R^2 \). \( DSS \) (Distributive Set Subfields) tests if \( D(\alpha, \beta) \), for a given pair \((\alpha, \beta) \in g^{[r]_0} H \times g^{[s]_0} H \) for some positive integers \( r, s \), can be considered as a subfield of \( \mathbb{F}_{q^n} \). The algorithm is described as follows:

**Algorithm 8.1.**

**Step 1: Dickson pair**

We define the function \( \text{isDicksonpair}(q, n) \). Note that \( \text{isDicksonpair}(q, n) \) returns True if \((q, n)\) is Dickson pair, false if it is not and list all Dickson pairs \((p^l, n)\) such that \((p, n, l) \in (1, x) \times (1, y) \times (1, z) \) where \( x, y \) and \( z \) are three positive integers.
Denote by $H$ the subgroup of $\mathbb{F}_{q^n}^*$ generated by $g^n$. Each non-zero element $\alpha$ of $\mathbb{F}_{q^n}^*$ is then in an $H$-coset of the form $g^{\frac{q^j-1}{q-1}}H$. The next function computes the value of $j$ in $\{0, 1, ..., n-1\}$ for $\alpha \in g^{\frac{q^j-1}{q-1}}H$.

**Step 2: Index of $H$-coset**

**Input:** An element $\alpha$ in $\mathbb{F}_{q^n}^*$.
**Output:** The index $j$ of $\alpha$ if it exists, false if it doesn’t.

define function isDicksonpair($q, n$)
1. $\mathbb{F}_{q^n}^* = \langle g \rangle$
2. define function associatedcoset($\alpha$)
3. if $\alpha \neq 0$
4. $\text{idx} = \log(\alpha, g)$ (return the logarithm of $\alpha$ to the base of $g$).
5. else return False
6. $\text{idx} = \text{idx} \mod (n)$ (since $H = \langle g^n \rangle$ we only care about $\text{idx}$ modulo $n$).
7. for $j \in \{0, ..., n\}$ do
8. $k = \frac{q^j-1}{q-1}$
9. $k = k \mod (n)$
10. if $\text{idx} = k$ then
11. return $j$

**Step 3: Matrix basis**

**Input:** $\alpha, \beta \in \mathbb{F}_{q^n}^*$.
**Output:** Basis for the space of solutions $\lambda$ to the equation $\phi(\lambda) = 0$. The idea is to perform this test on various randomly chosen $\alpha, \beta \in \mathbb{F}_{q^n}^*$.

1. define function $\phi(\alpha, \beta, \lambda, r, s, t)$
2. return $\alpha(\lambda^{q^j} - \lambda^r) - \beta(\lambda^{q^j} - \lambda^s)$
3. define function performtest($\alpha, \beta$)
4. $r = \text{associatedcoset}(\alpha)$
5. $s = \text{associatedcoset}(\beta)$
6. $t = \text{associatedcoset}(\alpha + \beta)$
7. if $r = s$ or $r = t$ or $s = t$ then
8. return ” $D(\alpha, \beta)$ is finite field”
9. else
10. for $j \in \{0, ..., n-1\}$ do
11. $M \leftarrow \text{matrix associated to } \phi(\alpha, \beta, g^j, r, s, t)$
12. $K \leftarrow \text{kernel } (M)$
13. if $\text{dim}(K) > 1$ then
14. return $K$
15. \textbf{if} isDicksonpair(q, n) \textbf{then}
16. \hspace{1em} \textbf{for} \ r_1 \in \{1, \ldots, q^n - 1\} \ \textbf{do}
17. \hspace{2em} \textbf{for} \ r_2 \in \{1, \ldots, q^n - 1\} \ \textbf{do}
18. \hspace{3em} \alpha \leftarrow g^{r_1}
19. \hspace{3em} \beta \leftarrow g^{r_2}
20. \hspace{2em} perform test(\alpha, \beta)

\textbf{Step 4: Row vector to field element}

\textbf{Input:} A row vector from the matrix basis \( K \) of \( D(\alpha, \beta) \) over \( \mathbb{F}_q \).
\textbf{Output:} Field element of \( D(\alpha, \beta) \).

1. define function \texttt{rowvectortofieldelement}(v)
2. \hspace{1em} a \leftarrow 0
3. \hspace{1em} k \leftarrow \text{number of column in } v \text{ (length (v)).}
4. \hspace{1em} \textbf{for} i \in \{1, \ldots k\}
5. \hspace{2em} a \leftarrow \sum_{i=1}^{k} v[i] \times g^{i-1}
6. \hspace{1em} \textbf{return} a

\textbf{Step 5: Field test}

1. define function \texttt{isfield}(K)
2. \hspace{1em} \textbf{if} dim(K) = 1 \ \textbf{then}
3. \hspace{2em} \textbf{return} True
4. \hspace{1em} \textbf{else}
5. \hspace{2em} B \leftarrow \text{set constituted by rows vectors in } K.
6. \hspace{2em} \textbf{for} i \in B \ \textbf{do}
7. \hspace{3em} \textbf{for} j \in B \ \textbf{do}
8. \hspace{4em} b_1 \leftarrow \texttt{rowvectortofieldelement}(i)
9. \hspace{4em} b_2 \leftarrow \texttt{rowvectortofieldelement}(j)
10. \hspace{4em} b \leftarrow b_1 b_2^{-1}
11. \hspace{3em} \textbf{if} row vector(b) \notin K \ \textbf{then}
12. \hspace{4em} \textbf{return} False

\textbf{Input:} \( K = \text{Kernel}(M) \).
\textbf{Output:} \( D(\alpha, \beta) \) is a finite field or not.

1. \textbf{if} isfield(K) \ \textbf{then}
2. \hspace{1em} \textbf{write} "\( D(\alpha, \beta) \) is a finite field".
3. \textbf{else}
4. \hspace{1em} \textbf{write} "\( D(\alpha, \beta) \) is not a finite field".


References

[1] J. ANDRÉ, Lineare Algebra über Fastkörpern, Mathematische Zeitschrift. 136 (1974), 295-313.
[2] JAMES C. BEIDLEMAN, On near-rings and near-ring modules. PhD thesis, Pennsylvania State University, 1966.
[3] CANNON, G ALAN AND FARAG, MARK AND KABZA, LUCYNA, Centers and generalized centers of near-rings Aequationes mathematicae, volume 68, 46-59, Springer, 2004.
[4] P. DJAGBA, K-T. HOWELL, The subspace structure of finite dimensional Beidleman near-vector spaces, Linear and Multilinear Algebra, accepted, to appear, https://doi.org/10.1080/03081087.2019.1582610, 2019.
[5] DICKSON LEONARD EUGENE, On finite algebras Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, 358-393, 1905.
[6] ERICH ELLERS UND HELMUT KARZEL, Endliche Inzidenzgruppen, Abhandl.Math.Seminar Hamburg 27 (1964): 250-264.
[7] AICHINGER, ERHARD AND FARAG, MARK, On when the multiplicative center of a near-ring is a subnear-ring, Communications in Algebra®, volume 35, 443-453, Taylor and Francis, 2007.
[8] SUSAN DANCs, The sub-near-field structure of finite near-fields, Bulletin of the Australian Mathematical Society 5.2 (1971): 275-280.
[9] SUSAN DANCs, On finite Dickson near-field, Abhandl.Math.Seminar Hamburg 37 (1972): 254-257.
[10] K-T HOWELL, Contributions to the Theory of Near-Vector Spaces, Ph.D.-dissertation, University of the Free State, 2008.
[11] HULL, THOMAS E AND DOBELL, ALAN R, Random number generators, SIAM review, volume 4, 230-254, SIAM, 1962.
[12] MEMLDRUM, JOHN DP, Near rings and their links with groups, Number 134, Pitman Advanced Publishing Program, 1985.
[13] PILZ GUNTER, Near-rings: the theory and its applications, volumes 23. Elsevier, 2011.
[14] WÄHLING, HEINZ, Theorie der Fastkörper, Thales Verlag, volume 1, 1987.
[15] H. ZASSENHAAUS, über endliche fastkörper. In Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, volume 11, pages 187–220. Springer, 1935.
[16] J.L. ZEMMER, Near-fields, planar and non-planar, The Math. Student 31 (1964): 145-150.