ISOMETRY AND AUTOMORPHISMS
OF CONSTANT DIMENSION CODES

ANNA-LENA TRAUTMANN
Institute of Mathematics
University of Zurich, Switzerland

(Communicated by Eimear Byrne)

Abstract. We define linear and semilinear isometry for general subspace codes, used for random network coding. Furthermore, some results on isometry classes and automorphism groups of known constant dimension code constructions are derived.

1. Introduction

Subspace codes are used for random linear network coding [1, 15]. They are defined as subsets of the projective geometry, which is the set of all subspaces of a given ambient space over a finite field. In the special case that all codewords have the same dimension, we call those codes constant dimension codes. It makes sense to define isometry classes of these codes and a canonical representative of each class to compare codes among each other.

On the other hand, a canonical form and the automorphism group are important for the theory of orbit codes [22], which are a special family of constant dimension codes. These codes are defined as orbits of a subgroup of the general linear group on an element of the projective geometry over a finite field. Different subgroups can possibly generate the same orbit, hence one needs a canonical way to compare orbit codes among each other. This can be done via the automorphism groups of the codes, since these are the maximal generating groups for a given orbit code and they contain all other generating subgroups of it.

The paper is structured as follows: We start with some preliminaries in Section 2. First we give some definitions and properties of concepts used for subspace coding. In the second part of the section we characterize linear and semilinear isometry of general subspace codes. As a main result we show that any (semi-)linearly isometric code of a given code can be obtained through the action of the projective (semi-)linear group.

In Section 3 we derive some theoretical results on and give some examples of isometry classes and automorphism groups of spread codes, orbit codes and lifted rank metric codes, which are known code constructions that will be explained in detail in that part.

We conclude in Section 4 by summing up the results.

2010 Mathematics Subject Classification: 11T71, 14G50.
Key words and phrases: Random network coding, projective space, finite fields, constant dimension codes, Grassmannian, isometries, automorphism groups.

The author is partially supported by Swiss National Science Foundation grant no. 138080 and Forschungskredit of the University of Zurich, grant no. 57104103.
2. Preliminaries

2.1. Subspace codes. Let \( \mathbb{F}_q \) be the finite field with \( q \) elements and the projective geometry \( \text{PG}(q, n-1) \) the set of all subspaces of \( \mathbb{F}_q^n \), whereas \( \mathcal{G}_q(k, n) \) is the set of all subspaces of \( \mathbb{F}_q^n \) of dimension \( k \), called Grassmannian. The general linear group \( \text{GL}_n(q) \) is the set of all invertible \( n \times n \)-matrices with entries in \( \mathbb{F}_q \).

\( \text{Aut}(\mathbb{F}_q) \) denotes the automorphism group of \( \mathbb{F}_q \). Recall that any automorphism \( \varphi \) of a finite field of characteristic \( p \) is of the type \( \varphi(x) = x^p \). It applies to vectors and matrices element-wise. Denote by \( \text{Gal}(\mathbb{F}_q^p, \mathbb{F}_q) \) the Galois group of \( \mathbb{F}_q^p \) over \( \mathbb{F}_q \), i.e. the set of all automorphisms of \( \mathbb{F}_q^p \) that stabilize the subfield \( \mathbb{F}_q \). It holds that \( \text{Aut}(\mathbb{F}_q^p) = \text{Gal}(\mathbb{F}_q^p, \mathbb{F}_q) \times \text{Aut}(\mathbb{F}_q) \). In particular, if \( p \) is the characteristic of \( \mathbb{F}_q \), then it holds that \( \text{Aut}(\mathbb{F}_q) = \text{Gal}(\mathbb{F}_q, \mathbb{F}_p) \).

The set of all semilinear mappings, i.e. the general semilinear group \( \Gamma \text{L}_n(q) := \text{GL}_n(q) \rtimes \text{Aut}(\mathbb{F}_q) \) decomposes as a semidirect product with the multiplication

\[
(A, \varphi)(B, \varphi') := (A \varphi^{-1}(B), \varphi\varphi').
\]

By \( \text{Mat}_{k \times n}(q) \) we denote the set of all \( k \times n \)-matrices with entries in \( \mathbb{F}_q \). If the underlying field is clear from the context we abbreviate the above by \( \text{GL}_n, \Gamma \text{L}_n \) and \( \text{Mat}_{k \times n} \), respectively.

Let \( U \in \text{Mat}_{k \times n} \) be a matrix of rank \( k \) and

\[
U = \text{rs}(U) := \text{row space}(U) \in \mathcal{G}_q(k, n).
\]

One notices that the row space is invariant under \( \text{GL}_k \)-multiplication on the left, i.e. for any \( T \in \text{GL}_k \)

\[
U = \text{rs}(U) = \text{rs}(TU).
\]

A unique representative of all matrices with the same row space is the one in reduced row echelon form. Any full-rank \( k \times n \)-matrix can be transformed into reduced row echelon form by a unique \( T \in \text{GL}_k \).

The subspace distance \( d_S \) and the injection distance \( d_I \) are metrics on the projective geometry \( \text{PG}(q, n-1) \) given by

\[
d_S(U, V) = \dim(U + V) - \dim(U \cap V)
\]

\[
= \dim(U) + \dim(V) - 2 \dim(U \cap V),
\]

\[
d_I(U, V) = \max\{\dim(U), \dim(V)\} - \dim(U \cap V),
\]

for any \( U, V \in \text{PG}(q, n-1) \). They are suitable distances for coding over the operator channel [15], where the injection metric is the more suitable one for an adversary model [18]. Since for \( U, V \in \mathcal{G}_q(k, n) \) it holds that

\[
d_S(U, V) = 2d_I(U, V),
\]

they are exchangeable in the study of constant dimension codes. If we do not need to specify which metric we are using we will write \( d(U, V) \).

In general a subspace code is simply a subset of \( \text{PG}(q, n-1) \). A constant dimension code is a subset of \( \mathcal{G}_q(k, n) \). The minimum distance of a code is defined in the usual way.

Bounds on the size of subspace codes can be found e.g. in [6, 13, 15]. Different constructions of constant dimension codes have been investigated in e.g. [5, 14, 15, 19, 20, 22].

Given \( U \in \text{Mat}_{k \times n} \) of rank \( k \), \( U \in \mathcal{G}_q(k, n) \) its row space and \( (A, \varphi) \in \Gamma \text{L}_n \), we define

\[
U(A, \varphi) := \text{rs}(\varphi(UA)).
\]
Since \( \varphi(TUA) = \varphi(T)\varphi(UA) \) for any \( T \in \text{GL}_k \), the operation here defined is independent from the representation of \( U \) and therefore well-defined. The \( \GammaL_n \)-multiplication defines a group action from the right on the Grassmannian and hence on \( \text{PG}(q, n-1) \) as well:

\[
\mathcal{G}_q(k, n) \times \GammaL_n \rightarrow \mathcal{G}_q(k, n)
\]

\[
(A, \varphi) \mapsto U(A, \varphi)
\]

This is indeed a group action since

\[
(UA)(B, \varphi)' = \varphi'(UA(B, \varphi)) = \varphi'(UA(\varphi^{-1}(B))) = \varphi(UA(\varphi^{-1}(B)), \varphi') = \varphi((A, \varphi)(B, \varphi')).
\]

It induces a group action of \( \text{GL}_n \) on \( \text{PG}(q, n-1) \), too.

This action respects the distances \( d_S, d_I \) and therefore may be used to define equivalence for subspace codes. In Section 2.2 we will show, that this equivalence is the most general one may demand if one also wants to preserve some other elementary properties of subspace codes.

Generally, group actions on sets are performed element-wise. For a group \( G \) acting from the right on a set \( X \) and an element \( x \in X \), \( \text{Stab}_G(x) := \{g \in G \mid xg = x\} \) denotes the stabilizer of \( x \) under \( G \). The orbit of \( x \in X \) under \( G \) is denoted by \( xG := \{xg \mid g \in G\} \) and the set of all orbits by \( X/G := \{xG \mid x \in X\} \). A transversal of \( X/G \) is a set containing one element of each orbit.

For the whole paper, if not stated differently, we will use vectors in row form and \( \GammaL_n \) and \( \text{GL}_n \) will be applied from the right.

We can now define linear and semilinear automorphisms of subspace codes.

**Definition 2.1.** The set

\[
\text{SAut}(C) := \text{Stab}_{\GammaL_n}(C) := \{(A, \varphi) \in \GammaL_n \mid C(A, \varphi) = C\}
\]

is a subgroup of \( \GammaL_n \) and is called the *semi-linear automorphism group* of the subspace code \( C \). The *linear automorphism group* of \( C \) is defined as

\[
\text{Aut}(C) := \text{Stab}_{\text{GL}_n}(C) := \{A \in \text{GL}_n \mid CA = C\}
\]

and is a subgroup of \( \text{SAut}(C) \).

**Lemma 2.2.** For a given subspace code \( C \subseteq \text{PG}(q, n-1) \) it holds that

\[
\lambda I_n \in \text{Aut}(C) \text{ for all } \lambda \in \mathbb{F}_q \setminus \{0\} =: \mathbb{F}_q^*.
\]

**Proof.** One can easily see that \( \lambda I_n \in \text{Aut}(U) \) for all \( U \in \text{PG}(q, n-1) \) and \( \lambda \in \mathbb{F}_q^* \). Then the statement follows from the fact that the pointwise stabilizer group is always a subset of the setwise stabilizer group.

\[ \square \]

**2.2. Isometry of Subspace Codes.** An open question is how to define equivalence of subspace codes. Naturally, equivalent codes should have the same ambient space, cardinality, error-correction capability (i.e. minimum distance) and transmission rate (for a fixed ambient space this is given by the maximal dimension of the codewords). Moreover, the distance distribution and the dimension distribution should be the same. Clearly, these last two conditions imply the minimum distance and maximum dimension.

This work engages in the equivalence maps of subspace codes that, in addition, preserve the dimensions of the codewords. In the following we will characterize all such maps.
Definition 2.3. A distance-preserving map $\iota : \text{PG}(q, n - 1) \to \text{PG}(q, n - 1)$ i.e. fulfilling
\[ d(U, V) = d(\iota(U), \iota(V)) \quad \forall U, V \in \text{PG}(q, n - 1). \]
is called an isometry on $\text{PG}(q, n - 1)$.

Any isometry $\iota$ is injective:
\[ U \neq V \iff d(U, V) \neq 0 \iff d(\iota(U), \iota(V)) \neq 0 \iff \iota(U) \neq \iota(V) \]
and hence, if the domain is equal to the co-domain, bijective. The inverse map $\iota^{-1}$ is an isometry as well.

Lemma 2.4. If $\iota : \text{PG}(q, n - 1) \to \text{PG}(q, n - 1)$ is an isometry, then $\iota(\{0\}) \in \{\{0\}, \mathbb{F}_q^n\}$.

Proof. We will prove it using the subspace distance. The proof for the injection distance is analogous.
Assume $U := \iota(\{0\}) \notin \{\{0\}, \mathbb{F}_q^n\}$ and let $V := \iota(\mathbb{F}_q^n)$. It holds that
\[ d_S(\{0\}, \mathbb{F}_q^n) = d_S(\iota(\{0\}), \iota(\mathbb{F}_q^n)) \]
\[ \iff n = d_S(U, V) \]
\[ \iff n = \dim(U + V) - \dim(U \cap V). \]
This implies $U + V = \mathbb{F}_q^n$ and $U \cap V = \{0\}$ and thus $V \notin \{\{0\}, \mathbb{F}_q^n\}$. Choose non-zero vectors $u \in U, v \in V$ and consider the one-dimensional subspace $W$ generated by $u + v$. Then $\dim(U \cap W) = \dim(V \cap W) = 0$ and
\[ d_S(\iota^{-1}(W), \{0\}) = d_S(W, U) = 1 + \dim(U), \]
\[ d_S(\iota^{-1}(W), \mathbb{F}_q^n) = d_S(W, V) = 1 + \dim(V), \]
which leads to the following contradiction (recall that $d_S(X, \{0\}) = \dim(X)$ and $d_S(X, \mathbb{F}_q^n) = n - \dim(X)$ for any $X \in \text{PG}(q, n - 1)$):
\[ n = d_S(\iota^{-1}(W), \{0\}) + d_S(\iota^{-1}(W), \mathbb{F}_q^n) = 2 + \dim(U) + \dim(V) = 2 + n. \]

We can use this fact to show that any isometry on $\text{PG}(q, n - 1)$ is either dimension-preserving or dimension-inverting, as shown in the following lemma.

Lemma 2.5. Let $\iota$ be as before and $U \in \text{PG}(q, n - 1)$ arbitrary. Then
\[ \iota(\{0\}) = \{0\} \Rightarrow \dim(U) = d(\{0\}, U) = d(\{0\}, \iota(U)) = \dim(\iota(U)), \]
and on the other hand
\[ \iota(\{0\}) = \mathbb{F}_q^n \Rightarrow \dim(U) = d(\{0\}, U) = d(\mathbb{F}_q^n, \iota(U)) = n - \dim(\iota(U)). \]

In the following, we restrict ourselves to the isometries with $\iota(\{0\}) = \{0\}$ because these are exactly the isometries that keep the dimension of a codeword. Now we want to characterize all these isometries on $\text{PG}(q, n - 1)$ with $\iota(\{0\}) = \{0\}$. For it we need the Fundamental Theorem of Projective Geometry:

Theorem 2.6 ([2, 3]). Let $Z_n := \{\mu I_n \mid \mu \in \mathbb{F}_q^*\}$ be the set of scalar transformations. Then every order-preserving bijection (with respect to the subset relation) $f : \text{PG}(q, n - 1) \to \text{PG}(q, n - 1)$, where $n > 2$, is induced by a semilinear transformation $(A, \varphi) \in \text{PGL}_n = (\text{GL}_n/Z_n) \rtimes \text{Aut}(\mathbb{F}_q)$. 

Advances in Mathematics of Communications
Volume 7, No. 2 (2013), 147–160
Theorem 2.7. For \( n > 2 \) a map \( \iota : \operatorname{PG}(q, n - 1) \to \operatorname{PG}(q, n - 1) \) is an order-preserving bijection (with respect to the subset relation) of \( \operatorname{PG}(q, n - 1) \) if and only if it is an isometry with \( \iota(\emptyset) = \emptyset \).

Proof. We will again prove the statement using the subspace distance, where an analogous proof holds for the injection distance.

1. \( \iota \) is an isometry with \( \dim(\emptyset) = 0 \).

Let \( \iota \) be an isometry with \( \iota(\emptyset) = \emptyset \). We have to show that for any \( U, V \in \operatorname{PG}(q, n - 1) \) the following holds:

\[ U \subseteq V \iff \iota(U) \subseteq \iota(V). \]

From Lemma 2.5 one knows that \( \dim(U) = \dim(\iota(U)) \). Assume that there are \( U, V \in \operatorname{PG}(q, n - 1) \) with \( U \subseteq V \) and \( \iota(U) \not\subseteq \iota(V) \). This leads to the contradiction:

\[ d_S(\iota(U), \iota(V)) = \dim(\iota(U)) + \dim(\iota(V)) - 2 \dim(\iota(U) \cap \iota(V)) \]
\[ > \dim(\iota(U)) + \dim(\iota(V)) - 2 \dim(\iota(U)) \]
\[ = \dim(U) + \dim(V) - 2 \dim(U) \]
\[ = \dim(U) + \dim(V) - 2 \dim(U \cap V) \]
\[ = d_S(U, V). \]

Hence \( U \subseteq V \implies \iota(U) \subseteq \iota(V) \). Since \( \iota^{-1} \) is an isometry as well, the converse also holds. Thus, \( \iota \) is an order-preserving bijection.

2. \( \iota \) is an isometry with \( \iota(\emptyset) = \emptyset \).

According to Theorem 2.6 any order-preserving bijection \( \iota \) of the projective geometry can be expressed by a pair \((A, \varphi) \in \operatorname{PTL}_n\). Then

\[ d_S(\iota(U), \iota(V)) = d_S(\varphi(UA), \varphi(VA)) \]
\[ = \dim(\varphi(UA)) + \dim(\varphi(VA)) - 2 \dim(\varphi(UA) \cap \varphi(VA)) \]
\[ = \dim(U) + \dim(V) - 2 \dim(\varphi(U \cap V)A) \]
\[ = d_S(U, V), \]

thus \( \iota \) is an isometry with \( \iota(\emptyset) = \emptyset \). \( \square \)

Corollary 2.8. Every isometry \( \iota \) on \( \operatorname{PG}(q, n - 1) \), where \( n > 2 \), with \( \dim(U) = \dim(\iota(U)) \) for any \( U \in \operatorname{PG}(q, n - 1) \) is induced by a semilinear transformation \((A, \varphi) \in \operatorname{PTL}_n\).

From now on assume that \( n > 2 \). This is no real restriction, because for application, subspace codes in an ambient space of dimension 2 are not interesting since the only non-trivial subspaces are the one-dimensional ones. In that case neither the transmission rate is improved compared to forwarding, nor is error-correction possible.

Definition 2.9. 1. Two codes \( C_1, C_2 \subseteq \operatorname{PG}(q, n - 1) \) are linearly isometric if there exists \( A \in \operatorname{PGL}_n := \operatorname{GL}_n / \mathbb{Z}_n \) such that \( C_1 = C_2A \). Since it is the orbit of \( \operatorname{PGL}_n \) on the code, the set of all linearly isometric codes is denoted by \( C_1\operatorname{PGL}_n \).

2. We call \( C_1 \) and \( C_2 \) semilinearly isometric if there exists \((A, \varphi) \in \operatorname{PTL}_n\) such that \( C_1 = C_2(A, \varphi) \). The set of all semilinearly isometric codes is denoted by \( C_1\operatorname{PTL}_n \).
Clearly linear and semilinear isometry are equivalence relations, so it makes sense to speak of classes of (semi-)linearily isometric codes. Note, that the isometries are independent of the underlying metric. Note furthermore, that one can replace the projective groups with $\text{GL}_n$ and $\Gamma\text{L}_n$, respectively, when computing the isometry classes of subspace codes (this follows from Lemma 2.2).

The interested reader can find a lattice point-of-view of the isometries of subspace codes in [21].

3. ISOMETRY AND AUTOMORPHISMS OF KNOWN CODE CONSTRUCTIONS

In this section we will examine the isometries and automorphism groups of some known classes of constant dimension codes, namely spread codes, orbit codes and lifted rank metric codes.

3.1. SPREAD CODES. Spreads of vector spaces are well-known geometrical objects, defined to be partitions of the non-zero elements of a given vector space into subspaces (without the zero-element) of that vector space of a fixed dimension. I.e. a $k$-spread of $\mathbb{F}^n_q$ is a set of subspaces of dimension $k$ such that they pairwise intersect only trivially and they cover the whole vector space $\mathbb{F}^n_q$. Thus, a spread exists if and only if $k|n$ and is a subset of $\mathcal{G}_q(k,n)$, i.e. it can be used as a constant dimension code. In this case we speak of a spread code. A spread code has cardinality $(q^n-1)/(q^k-1)$ and minimum subspace distance $2k$.

Different constructions for these codes are known and have been studied from a coding perspective, e.g. in [9, 16, 17].

The trivial cases are $k=1$ where the spread corresponds to the projective space and $k=n$ where the spread has one element, namely the whole space.

One way of constructing spreads is the $\mathbb{F}_q^k$-linear representation of $\mathbb{F}_q^n$ (cf. e.g. [11, ch. 4]): Since $k|n$ we can consider $\mathbb{F}_q^n$ as an extension field of $\mathbb{F}_q^k$ of degree $l:=n/k$, which is isomorphic to the vector space $\mathbb{F}_q^l$. In this vector space consider the trivial spread of all one-dimensional subspaces. Each of these lines over $\mathbb{F}_q^l$ can now be considered as a $k$-dimensional subspace over $\mathbb{F}_q$. Since the lines of $\mathbb{F}_q^l$ intersect only trivially and with a simple counting argument it follows that the corresponding $k$-dimensional subspaces of $\mathbb{F}_q^n$ form a spread.

We call a spread code Desarguesian if it is an $\mathbb{F}_q^k$-linear representation of $\mathbb{F}_q^n$, or if it is a column permutation of such a code.

**Theorem 3.1.** All Desarguesian spread codes are linearly isometric.

**Proof.** Since there is only one spread of lines in $\mathbb{F}_q^k$, different Desarguesian spreads of $\mathbb{F}_q^n$ can only arise from the different isomorphisms between $\mathbb{F}_q^k$ and $\mathbb{F}_q^n$. As the isomorphisms are linear maps, there exists a linear map between the different spreads arising from them.

In general, not all spreads are linearly isometric but in the special case of $q=2$, $k=2$, $n=4$ they actually are:

**Proposition 3.2.** All spreads in $\mathcal{G}_2(2,4)$ are linearly isometric.

**Proof.** To prove the statement we need the following definitions from [10]: A transversal of $\mathcal{U}$ in $\mathcal{G}_q(2,4)$ is an element $\mathcal{V} \in \mathcal{G}_q(2,4)$ such that $\dim(\mathcal{U} \cap \mathcal{V}) = 1$. The set of transversals of three elements of $\mathcal{G}_q(2,4)$ is called a regulus. A spread $\mathcal{S} \subset \mathcal{G}_q(2,4)$ is called regular if, when $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3 \in \mathcal{S}$, then the regulus of $\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3$ is contained in $\mathcal{S}$.
From [10, Lemma 17.1.3] we know that every spread in $G_q(2,4)$ is regular. Since in $G_2(k,2k)$ a spread is Desarguesian if and only if it is regular [12, p. 207], we know that every spread is Desarguesian. Hence all spreads in $G_2(2,4)$ are linearly isometric. 

We will now investigate the automorphism groups of Desarguesian spreads.

**Theorem 3.3.** Let $C \subseteq G_q(k,n)$ be a Desarguesian spread code. Then the linear automorphism group of $C$ is isomorphic to $GL_\mathbb{F}_q(q^k) \times \operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.

**Proof.** Let $l := n/k$. We want to find all $\mathbb{F}_q$-linear bijections of $\mathbb{P}^{l-1}(\mathbb{F}_{q^k})$. We know that $\operatorname{PGL}_l(q^k)$ is the groups of all $\mathbb{F}_{q^k}$-linear bijections of $\mathbb{P}^{l-1}(\mathbb{F}_{q^k})$. Thus, $\operatorname{PGL}_l(q^k) \times \operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$ is the set of all $\mathbb{F}_q$-linear bijections of $\mathbb{P}^{l-1}(\mathbb{F}_{q^k})$. It follows that non-projectively the linear automorphism group of such a spread is isomorphic to $GL_l(q^k) \times \operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$. 

**Corollary 3.4.** Let $S$ be a Desarguesian spread code in $G_q(k,n)$. Then

$$|\operatorname{Aut}(S)| = k \prod_{i=0}^{\frac{n}{k}-1} q^n - q^{ki}.$$ 

**Proof.** Follows from the fact that $|\operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)| = k$ and

$$|GL_\mathbb{F}_q(q^k)| = \prod_{i=0}^{\frac{n}{k}-1} (q^k)^i - (q^k)^i.$$ 

Since we would like to represent the finite field automorphisms as invertible matrices we need the following lemma:

**Lemma 3.5.** Let $\phi : \mathbb{F}_q^k \rightarrow \mathbb{F}_{q^k}$ be a vector space isomorphism and $\varphi \in \operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$. Then there exists a matrix $A \in \operatorname{GL}_k$ such that

$$\phi(vA) = \varphi(v).$$

I.e. there is a matrix-representation in $\operatorname{GL}_k$ for every element of $\operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.

**Proof.** Follows from the fact that $\varphi$ is linear and that $\mathbb{F}_q^k$ is isomorphic to $\mathbb{F}_{q^k}$. 

We can now translate the result of Corollary 3.4 to a matrix setting. Since $\mathbb{F}_{q^k}$ is isomorphic to $\mathbb{F}_q[\alpha]$ where $\alpha$ is a root of an monic irreducible polynomial $p(x) \in \mathbb{F}_q[x]$ of degree $k$ but also to $\mathbb{F}_q[P]$ where $P$ the companion matrix of $p(x)$, we get:

**Corollary 3.6.** The automorphism group of a Desarguesian spread code in $G_q(k,n)$ is generated by all elements in $\operatorname{GL}_n$ where the $k \times k$-blocks are elements of $\mathbb{F}_q[P]$ and block diagonal matrices where the blocks represent an element of $\operatorname{Gal}(\mathbb{F}_{q^k}, \mathbb{F}_q)$.

Another point of view of the construction of a Desarguesian spread can be found in [16], where the generator matrices of the code words are of the type

$$U = \begin{bmatrix} B_1 & B_2 & \ldots & B_l \end{bmatrix}$$

where the blocks $B_i$ are an element of $\mathbb{F}_q[P]$ and $P$ is a companion matrix of an irreducible polynomial of degree $k$. To stay inside this structure (i.e. to apply an automorphism) we can permute the blocks, do block-wise multiplications or do block-wise additions with elements from $\mathbb{F}_q[P]$. This coincides with the structure of the automorphism groups from before.

This result is depicted in the following Examples.
Example 3.7. Consider $G_2(2, 4)$. The only binary irreducible polynomial of degree 2 is $p(x) = x^2 + x + 1$, i.e. 

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. $$

The respective spread code is 

$$C = \{ rs \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}, rs \begin{bmatrix} I & I \\ I & P \end{bmatrix}, rs \begin{bmatrix} I & P^2 \\ I & I \end{bmatrix}, rs \begin{bmatrix} 0 & I \\ I & P \end{bmatrix}, rs \begin{bmatrix} 0 & I \\ I & P \end{bmatrix} \}$$

and its automorphism group has 360 elements:

$$\text{Aut}(C) = \langle \left( \begin{pmatrix} I & I \\ I & P \end{pmatrix}, \left( \begin{pmatrix} I & I \\ I & P \end{pmatrix}, \left( Q \right) \right) \right) \rangle$$

where $Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2$ represents the only non-trivial automorphism of $\mathbb{F}_{2^2}$, i.e. $x \mapsto x^2$.

A different approach of finding the automorphism group of a spread in $G_2(2, 4)$ can also be found in [10, Corollary 2].

Example 3.8. Consider $G_3(2, 4)$ and the irreducible polynomial $p(x) = x^2 + x + 2$, i.e. 

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}. $$

The spread code is 

$$C = \{ rs \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix} \cup \{ rs \begin{bmatrix} I & P^i \\ i = 0, \ldots, 7 \} \cup rs \begin{bmatrix} 0 & I \\ I & P \end{bmatrix} \cup rs \begin{bmatrix} 0 & I \\ I & P \end{bmatrix} \cup rs \begin{bmatrix} 0 & I \\ I & P \end{bmatrix} \cup rs \begin{bmatrix} 0 & I \\ I & P \end{bmatrix} \}$$

and its automorphism group has 11520 elements:

$$\text{Aut}(C) = \langle \left( \begin{pmatrix} I & I \\ I & P \end{pmatrix}, \left( \begin{pmatrix} I & I \\ I & P \end{pmatrix}, \left( Q \right) \right) \right) \rangle$$

where $Q = \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} \in \text{GL}_2$. Here $Q$ represents the only non-trivial automorphism of $\mathbb{F}_{3^2}$, i.e. $x \mapsto x^3$.

Note, that in both examples the first element of the generator sets corresponds to swapping the blocks, the second corresponds to multiplication by $P$ and the third element to adding $P$ in the second block of the code word generator matrices.

To conclude this subsection we want to give an example of a non-Desarguesian spread and show that its automorphism group has a different cardinality than the ones of a Desarguesian spread of the same parameters.

Example 3.9. In the setting of Example 3.8, one can construct a non-Desarguesian spread as follows:

$$C' = \{ rs \begin{bmatrix} I & P^i \\ i \in \{ 0, 2, 3, 4, 6, 7 \} \} \cup rs \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cup rs \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{bmatrix} \cup \{ rs \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cup rs \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \}.$$

We used the algorithm of [7] to compute its automorphism group, and got a group of size

$$|\text{Aut}(C')| = 3840$$

which is a third of the size of the automorphism group of the Desarguesian spread in Example 3.8. This implies that $C$ and $C'$ are not linearly isometric.
3.2. Orbit codes. Orbit codes are defined as orbits under the group action of the general linear group on the Grassmannian, i.e. a code \( C \subseteq G_q(k, n) \) is an orbit code if it can be written as \( UC \), where \( U \in G_q(k, n) \) and \( G \leq GL_n \). We say that \( G \) is a generating group of \( C \). These codes were first defined in [22]. For more information on orbit codes the reader is referred to [21], where also a similar version of the following fact on isometry of orbit codes can be found:

**Theorem 3.10.** Let \( C_1 = U_1G \) be an orbit code. Then \( C_2 \) is linearly (respectively semilinearly) isometric to \( C_1 \) if and only if there exists \( S \in GL_n \) (respectively \( S \in PGL_n \)) such that

\[
C_2 = U_1S(S^{-1}GS),
\]

i.e. \( S^{-1}GS \) is a generating group of \( C_2 \). Hence, the isometry classes of orbit codes in \( G_q(k, n) \) correspond to the conjugacy classes of the subgroups of \( GL_n \).

One natural question that arises when studying orbit codes is if there is a canonical representative of all the possible generating groups for a given orbit code. The following proposition shows that the automorphism groups can function as such representatives, since they are always the largest generating group of a given code.

**Proposition 3.11.**

1. Every generating group of an orbit code is a subgroup of the automorphism group.
2. Every subgroup of the automorphism group containing a generating group is a generating group. Hence, the automorphism group is a generating group of the orbit code.

**Proof.**

1. If \( C = UG \), then \( CG = UGG = UG \).
2. Let \( G \) be a generating group of \( C \) and \( G \leq H \leq \text{Aut}(C) \). Hence, \( C = UG \) and \( CH = C \). This implies that \( UH = UGH = CH = C \), since \( G \) is a subgroup of \( H \).

The question of finding elements of the automorphism group can be translated into a stabilizer condition of the initial point of the orbit.

**Proposition 3.12.** \( A \in GL_n \) is in the automorphism group of \( C = UG \) if and only if for every \( B' \in G \) there exists a \( B'' \in G \) such that

\[
B'AB'' \in \text{Stab}_{GL_n}(U).
\]

**Proof.** We have

\[
A \in \text{Aut}(C) \iff CA = C \\
\iff \forall B' \in G \exists B^* \in G : UB'A = UB^* \\
\iff \forall B' \in G \exists B^* \in G : UB'BA^{-1} = U.
\]

The statement follows with \( B'' := B^*^{-1} \in G \).

3.3. Lifted rank-metric codes. In this subsection we want to study the isometries and automorphisms of lifted rank-metric codes. To do so we will first recall the definition of rank-metric codes and known results about the isometries of these codes. Then we will recall the definition of lifted rank-metric codes and then use the before mentioned results to investigate the isometries of lifted rank-metric codes. Moreover, we will show the connection between the automorphism groups of rank-metric and lifted rank-metric codes.
Rank-metric codes are matrix codes, i.e. subsets of $\text{Mat}_{k \times m}$ (in this work we will restrict ourselves to the case $k \leq m$) equipped with the rank distance
\[ d_R(U, V) := \text{rank}(U - V) \quad \text{for } U, V \in \text{Mat}_{k \times m}. \]
Such a matrix code can also be seen as a block code in $\mathbb{F}_q^m$, where the code words are column vectors of length $k$. We will denote rank-metric codes by $\mathcal{C}_R$. For more information on rank-metric codes the reader is referred to [8].

The isometry of rank-metric codes (as block codes over $\mathbb{F}_q^m$) has already been studied by Berger in [4]. One of his main results is the following:

**Lemma 3.13 ([4]).**

1. The set of $\mathbb{F}_q^m$-linear isometries on $\mathbb{F}_q^k$ equipped with the rank metric is
   \[ R^{\text{lin}}(\mathbb{F}_q^m) := \text{GL}_k(q) \times \mathbb{F}_q^m. \]

2. The set of $\mathbb{F}_q^m$-semilinear isometries on $\mathbb{F}_q^k$ equipped with the rank metric is
   \[ R^{\text{semi}}(\mathbb{F}_q^m) := (\text{GL}_k(q) \times \mathbb{F}_q^m) \rtimes \text{Aut}(\mathbb{F}_q^m). \]

Since we are interested in the matrix representation of these codes and hence also their isometries, let us now translate the previous result to a matrix setting:

**Corollary 3.14.** Let $p(x) = \sum_{i=0}^m p_i x^i \in \mathbb{F}_q[x]$ be monic and irreducible of degree $m$ and $P \in \text{GL}_m(q)$ its companion matrix. Let $\alpha \in \mathbb{F}_q^m \cong \mathbb{F}_q[m]$. Denote by $\text{Gal}_M(\mathbb{F}_q[m]) \leq \text{GL}_m(q)$ the matrix representation of $\text{Gal}(\mathbb{F}_q[m], \mathbb{F}_q)$ (as illustrated in Lemma 3.5 and Examples 3.7 and 3.8). Then the following holds:

1. The set of $\mathbb{F}_q[m]$-linear isometries on $\text{Mat}_{k \times m}$ equipped with the rank metric is $\text{GL}_k(q) \times \mathbb{F}_q^m[P]$.
2. The set of $\mathbb{F}_q[m]$-semilinear isometries on $\text{Mat}_{k \times m}$ equipped with the rank metric is $(\text{GL}_k(q) \times \mathbb{F}_q^m[P]) \rtimes (\text{Gal}_M(\mathbb{F}_q^m) \times \text{Aut}(\mathbb{F}_q^m))$.

Here $\text{GL}_k$ always acts from the left and $\mathbb{F}_q^m[P]$ as well as $\text{Gal}_M(\mathbb{F}_q^m)$ always act from the right when applied to an element of $\text{Mat}_{k \times m}$.

**Proof.** Denote by $\phi : \mathbb{F}_q^m \to \mathbb{F}_q[m]$ the isomorphism between the vector space and the extension field of degree $m$. It is well-known that the following holds (cf. e.g. [21]) for any $v \in \mathbb{F}_q^m$:
\[ \phi(NP) = \phi(v)\alpha. \]
Since $\mathbb{F}_q[m]$ is isomorphic to $\mathbb{F}_q[P]$, we get that multiplying an element of $\mathbb{F}_q^m$ by $\sum_{i=0}^{m-1} \beta_i \alpha^i \in \mathbb{F}_q[m]$ is isomorphic to multiplying the respective element of $\text{Mat}_{k \times m}$ with $\sum_{i=0}^{m-1} \beta_i P^i \in \mathbb{F}_q[P]$. Then, together with Lemma 3.13, the first statement follows. The second statement is implied by the fact that $\text{Aut}(\mathbb{F}_q^m) = \text{Gal}(\mathbb{F}_q^m, \mathbb{F}_q) \times \text{Aut}(\mathbb{F}_q)$.

Note, that an $\mathbb{F}_q[m]$-linear map is also $\mathbb{F}_q$-linear. On the other hand, there are other $\mathbb{F}_q$-(semi)-linear isometries than the ones mentioned before. E.g. all elements of $\text{GL}_m$ are $\mathbb{F}_q$-linear isometries on $\text{Mat}_{k \times m}$, since they are rank-preserving.

One can create constant dimension codes from a given rank-metric code, as explained in the following.

**Lemma 3.15 ([19]).** Let $\mathcal{C}_R \subseteq \text{Mat}_{k \times n-k}$ be a rank-metric code with minimum distance $d$. Then the lifted code
\[ C = \{ rs[I_k \ R] \mid R \in \mathcal{C}_R \} \]
is a constant dimension code in $\mathcal{G}_q(k, n)$ with minimum distance $2d$. 

**Advances in Mathematics of Communications Volume 7, No. 2 (2013), 147–160**
Since we usually study the case where \( n \geq 2k \) this construction justifies the restriction \( k \leq m \) (for the matrix size) from above.

We will now show the connection between the isometries of rank-metric codes and their lifted subspace codes.

**Theorem 3.16.** If two rank-metric codes in \( \text{Mat}_{k \times n-k} \) are \( \mathbb{F}_{q^n-k} \)-linearly (respectively \( \mathbb{F}_{q^n-k} \)-semilinearly) isometric in the rank-metric space, their lifted codes are linearly (respectively semilinearly) isometric in the Grassmannian \( G_{q}(k,n) \).

**Proof.** For simplicity we will first prove the statement for linearly isometric codes: Let \( C_R \) and \( C'_R \) be two \( \mathbb{F}_{q^n-k} \)-linearly isometric rank-metric codes, i.e. \( C'_R = AC_RP' \) with \( A \in \text{GL}_k \) and \( P' \in \mathbb{F}_q[P] \), where \( P \) is the companion matrix of a monic irreducible polynomial in \( \mathbb{F}_q[x] \) of degree \( n-k \). Then the lifted code of \( C'_R \) is

\[
C' = \{ rs \begin{bmatrix} I_k & R' \end{bmatrix} \mid R' \in C'_R \} = \{ rs \begin{bmatrix} I_k & ARP' \end{bmatrix} \mid R \in C_R \}
\]

\[
= \{ rs \begin{bmatrix} A^{-1} & R \end{bmatrix} \mid R \in C_R \} \left( \begin{bmatrix} I_k & P' \end{bmatrix} \right) = \{ rs \begin{bmatrix} I_k & R \end{bmatrix} \mid R \in C_R \} \left( A^{-1} P' \right)
\]

where \( C \) is the lifted code of \( C_R \). Hence, the lifted codes are linearly isometric.

The semi-linear case then follows together with Corollary 3.14, since an element from \( \text{Gal}_M(\mathbb{F}_{q^n-k}) \) behaves analogously to \( P' \) in the proof. \( \square \)

One can easily see, that there are codes that are linearly isometric to a lifted rank-metric code but are not a lifted rank-metric code itself:

**Example 3.17.** Consider the binary lifted rank-metric code

\[
C = \left\{ rs \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, rs \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \right\}.
\]

Permute the second and third column of both codewords to get

\[
C' = \left\{ rs \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, rs \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \right\}.
\]

Then \( C \) and \( C' \) are linearly isometric but \( C' \) is not a lifted rank-metric code.

We now want to investigate which isometries map a lifted rank-metric code to another lifted rank-metric code of the same parameters. Note, that it does not make sense to think of \( \mathbb{F}_{q^n-k} \)-linear isometry for the lifted codes, which is why we only study the \( \mathbb{F}_q \)-linear isometries.

**Theorem 3.18.** Let \( C_R \subseteq \text{Mat}_{k \times n-k} \) be an arbitrary rank-metric code with minimum distance \( d \). The following elements map \( C_R \) to another lifted rank-metric code in \( \text{Mat}_{k \times n-k} \) with the same minimum distance \( d \) and are semilinear isometries:

\[
\left\{ \left( \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \varphi \right) \mid A \in \text{GL}_k, C \in \text{GL}_{n-k}, B \in \text{Mat}_{k \times n-k}, \varphi \in \text{Aut}(\mathbb{F}_q) \right\}.
\]

For \( \varphi = \text{id} \) they are linear isometries.

**Proof.** Consider \( R, R' \in C_R \). With the block matrix multiplication rules it follows that

\[
rs \begin{bmatrix} I_k & R \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = rs \begin{bmatrix} A & B + RC \end{bmatrix} = rs \begin{bmatrix} I_k & A^{-1}(B + RC) \end{bmatrix}.
\]
From Corollary 3.14 we know that $A^{-1}$ is a rank-metric isometry. Moreover

$$\text{rank}((B + RC) - (B + R'C)) = \text{rank}((R - R')C) = \text{rank}(R - R'),$$

thus $\{A^{-1}(B + RC) \mid R \in CR\} \subseteq \text{Mat}_{k \times n-k}$ is a rank-metric code with the same minimum distance as $CR$. As $A$ and $C$ are invertible, the whole matrix $\begin{pmatrix} A & B \\ C \end{pmatrix}$ is in $GL_n$ and the statement follows.

Note, that with the notation from the preceding theorem the map

$$\text{Mat}_{k \times m} \rightarrow \text{Mat}_{k \times m}, \quad R \mapsto A^{-1}(B + RC)$$

is indeed an isometry but it is not linear, except for the case when $A^{-1}B = 0_{k \times n-k}$, which is equivalent to $B = 0_{k \times n-k}$, since $A \in GL_k$. Thus, the elements that map a lifted linear rank-metric code to another lifted linear rank-metric code of the same parameters have to fulfill $B = 0_{k \times n-k}$, in addition.

In the following we will focus on automorphisms of lifted rank-metric codes. We can again use the knowledge of the automorphism group of a rank-metric code for finding the automorphism group of the respective lifted rank-metric code. For this denote by $\text{Aut}_R$ the automorphism group of the rank-metric code.

**Proposition 3.19.** Let $\mathcal{C}_R \subseteq \text{Mat}_{k \times (n-k)}$ be a rank-metric code and $\mathcal{C}$ its lifted code. Then

$$\left\{ \begin{pmatrix} I_k \\ R \end{pmatrix} \mid R \in \text{Aut}_R(\mathcal{C}_R) \right\} \subseteq \text{Aut}(\mathcal{C}).$$

**Proof.** It holds that

$$\left\{ \left[ \begin{array}{c} I_k \\ B \end{array} \right] \mid B \in \mathcal{C}_R \right\} \begin{pmatrix} I_k \\ R \end{pmatrix} = \left\{ \left[ \begin{array}{c} I_k \\ BR \end{array} \right] \mid B \in \mathcal{C}_R \right\}.$$ 

Since $R \in \text{Aut}_R(\mathcal{C}_R)$, this set is equal to the original one. \qed

**Theorem 3.20.** Let $\mathcal{C}_R \subseteq \text{Mat}_{k \times (n-k)}$ be a rank-metric code and $\mathcal{C}$ its lifted code. Then

$$\left\{ \begin{pmatrix} I_k \\ A \end{pmatrix} \mid A \in \text{GL}_{n-k} \right\} \cap \text{Aut}(\mathcal{C}) = \left\{ \begin{pmatrix} I_k \\ R \end{pmatrix} \mid R \in \text{Aut}_R(\mathcal{C}_R) \right\}.$$ 

**Proof.** From Proposition 3.19 we know that the right side is included in the left. Furthermore,

$$\text{rs} \begin{pmatrix} I_k \\ B_1 \end{pmatrix} \begin{pmatrix} I_k \\ A \end{pmatrix} = \text{rs} \begin{pmatrix} I_k \\ B_2 \end{pmatrix}$$

$$\iff \exists C_1, C_2 \in \text{GL}_k : \left[ \begin{array}{c} C_1 \\ C_1B_1 \end{array} \right] \begin{pmatrix} I_k \\ A \end{pmatrix} = \left[ \begin{array}{c} C_2 \\ C_2B_2 \end{array} \right]$$

$$\iff C_1 = C_2 \quad \text{and} \quad B_1A = B_2$$

i.e. if $\begin{pmatrix} I_k \\ A \end{pmatrix} \in \text{Aut}(\mathcal{C})$, then $A \in \text{Aut}_R(\mathcal{C}_R)$. \qed

Hence, if we know the automorphism group of a lifted rank-metric code, we also know the automorphism group of the rank-metric code itself.
Example 3.21. Consider the rank-metric code

\[ \mathcal{C}_R = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \} \]

with four elements and minimum rank distance 1 over \( \mathbb{F}_2 \). Its automorphism group is

\[ \text{Aut}_R(\mathcal{C}_R) = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_2 \} \]

Let \( \mathcal{C} \) be the lifted code of \( \mathcal{C}_R \) in \( G_2(2, 4) \). Then

\[ \text{Aut}(\mathcal{C}) = \langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rangle \]

with \( |\text{Aut}(\mathcal{C})| = 192 \). The second generator and the identity matrix are the corresponding elements described in Theorem 3.20.

Note, that \( \text{Aut}_R(\mathcal{C}_R) \) can easily be found since \( |\text{GL}_2| = 6 \), while \( \text{Aut}(\mathcal{C}) \) was found by computer search, using the algorithm of [7].

4. Conclusion

In this work we investigated linear and semilinear isometry, as well as linear and semilinear automorphism groups, for general network codes, i.e. sets of vector spaces over a finite field. We showed that the subset-relation-and-dimension-preserving isometries correspond exactly to the general (semi-)linear group.

In Section 3 we showed some theoretical results and examples of isometry classes and automorphism groups of some known constructions of constant dimension codes, namely spread codes, orbit codes and lifted rank metric codes.

The isometry classes indicate how many non-equivalent different codes for given size and minimum distance can be found. On the other hand, the automorphism groups are useful for counting how many different codes there are in the same isometry class of a given code.

Moreover, the automorphism groups of orbit codes function as a canonical generating group to compare orbit codes among each other.

More research can be done in finding theoretical results on the automorphism groups of constant dimension codes. E.g. one could study the automorphism groups of non-Desarguesian spreads or try to find a family of orbit codes that have a certain automorphism group. Moreover, one could study the isometry and automorphism groups of non-constant dimension codes.

In general, it might not always be possible to determine the automorphism group of an arbitrary subspace code or check if two given codes are isometric with the results presented in this work. In that case, the algorithm of T. Feulner in [7] can be used to do these computations.

For future work it would be interesting to see how the knowledge of the automorphism group of a given constant dimension code (or a general subspace code) can be helpful for decoding, as it is in the classical block code case.
ACKNOWLEDGMENTS

The author thanks Thomas Feulner, without whom this work would not have been possible, as well as Joachim Rosenthal and Leo Storme for their advice. She would also like to thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, Network information flow, IEEE Trans. Inform. Theory, 46 (2000), 1204–1216.
[2] E. Artin, Geometric algebra, in “Interscience Tracts in Pure and Applied Mathematics,” John Wiley & Sons, 1988.
[3] R. Baer, Linear algebra and projective geometry, in “Pure and Applied Mathematics,” Academic Press, 1952.
[4] T. P. Berger, Isometries for rank distance and permutation group of gabidulin codes, IEEE Trans. Inform. Theory, 49 (2003), 3016–3019.
[5] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, IEEE Trans. Inform. Theory, 55 (2009), 2909–2919.
[6] T. Etzion and A. Vardy, Error-correcting codes in projective space, in “IEEE International Symposium on Information Theory,” (2008), 871–875.
[7] T. Feulner, Canonical forms and automorphisms in the projective space, preprint, 2012.
[8] E. M. Gabidulin, Theory of codes with maximum rank distance, Problemy Peredachi Informatsii, 21 (1985), 3–16.
[9] E. Gorla, F. Manganiello and J. Rosenthal, An algebraic approach for decoding spread codes, Adv. Math. Commun., 6 (2012), 443–466.
[10] J. W. P. Hirschfeld, “Finite Projective Spaces of Three Dimensions,” The Clarendon Press, Oxford University Press, New York, 1985.
[11] J. W. P. Hirschfeld, “Projective Geometries over Finite Fields,” 2nd edition, The Clarendon Press, Oxford University Press, New York, 1998.
[12] J. W. P. Hirschfeld and J. A. Thas, “General Galois Geometries,” The Clarendon Press, Oxford University Press, New York, 1991.
[13] A. Khaleghi, D. Silva and F. R. Kschischang, Subspace codes, in “IMA Int. Conf.”, (2009), 1–21.
[14] A. Kohnert and S. Kurz, Construction of large constant dimension codes with a prescribed minimum distance, in “Mathematical Methods in Computer Science,” Springer, Berlin, (2008), 31–42.
[15] R. Kötter and F. R. Kschischang, Coding for errors and erasures in random network coding, IEEE Trans. Inform. Theory, 54 (2008), 3579–3591.
[16] F. Manganiello, E. Gorla and J. Rosenthal, Spread codes and spread decoding in network coding, in “Proceedings of the 2008 IEEE International Symposium on Information Theory,” Toronto, (2008), 851–855.
[17] F. Manganiello and A.-L. Trautmann, Spread decoding in extension fields, preprint, arXiv:1108.5881
[18] D. Silva and F. R. Kschischang, On metrics for error correction in network coding, IEEE Trans. Inform. Theory, 55 (2009), 5479–5490.
[19] D. Silva, F. R. Kschischang and R. Kötter, A rank-metric approach to error control in random network coding, IEEE Trans. Inform. Theory, 54 (2008), 3951–3967.
[20] V. Skachek, Recursive code construction for random networks, IEEE Trans. Inform. Theory, 56 (2010), 1378–1382.
[21] A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, Cyclic orbit codes, preprint, arXiv:1112.1238
[22] A.-L. Trautmann, F. Manganiello and J. Rosenthal, Orbit codes - a new concept in the area of network coding, in “IEEE Information Theory Workshop (ITW),” Dublin, (2010), 1–4.

Received for publication June 2012.

E-mail address: trautmann@math.uzh.ch

Advances in Mathematics of Communications Volume 7, No. 2 (2013), 147–160