Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 209–214*

Geometrically Uniform n-shot Subspace Codes

Leandro Bezerra de Lima leandro.lima@ufms.br
CPAq/UFMS, Aquidauana, MS, Brasil - FEEC-UNICAMP, Campinas-SP, Brasil
Reginaldo Palazzo Junior palazzo@de.fee.unicamp.br
FEEC - Universidade Estadual de Campinas - UNICAMP, Campinas-SP, Brasil

Abstract. In [3] it is proposed an efficient error-control procedure for use in Network Coding called subspace codes constructed from projective space of order m over a finite field $\mathbb{F}_q$, denoted by $\mathbb{P}(\mathbb{F}_q^m)$, that is, the set of all subspaces in the vector space $\mathbb{F}_q^m$, [1]. The projective space endowed with the subspace metric is a metric space. Such subspace codes are devised for the one use of the channel. An alternative to improve the rate and the error-correcting capabilities, without increasing the order of the finite field or the vector length is to make use of the channel n times, this new code is known as the n-shot subspace code, [6]. In this paper we present the concept of geometrically uniform subspace codes and the new n-shot geometrically uniform subspace codes.

1 Introduction

The concept of geometrically uniform (GU) codes was introduced by Forney in [2]. This class of codes generalizes the Slepian type of codes and the lattice codes by allowing the elements of the group be arbitrary isometries. From the introduction of this class of codes several studies were realized, for instance in [4] the authors extended the concepts of GU codes to the hyperbolic context. Regarding the context of GU subspace codes, we mention the work of Akemi and Palazzo, [5], where an algorithm to construct GU subspace codes in a Grassmannian was proposed. In this paper we establish the conditions under which GU subspace codes for n-shot channels may be constructed.

2 Preliminaries

2.1 Geometrically uniform codes

In this subsection, the definitions and results related to GU codes are borrowed from [2]. For further details we refer the reader to [2].

Definition 2.1. *Let M be a metric space with metric d, and T be a transformation in M. T is an **isometry** if T preserves distance, that is, for every $x, y \in M$ we have that $d(x, y) = d(T(x), T(y))$.*

Definition 2.2. *A geometric figure S is a set of points in $\mathbb{R}^n$. Two figures S_1 and S_2 are **geometrically congruents** if there exists an isometry U in $\mathbb{R}^n$ such that $U(S_1) = S_2$.*

Definition 2.3. *An S-invariant isometry $U \in \mathbb{R}^n$, that is, $U(S) = S$ is called a* ***symmetry*** *of S.*

Observation 2.1. *The symmetries of S form a group under the operation of composition of functions, called* ***symmetry group*** *of S, and denoted by $\Gamma(S)$.*

Definition 2.4. *A signal set S is* ***geometrically uniform (GU)*** *if given any two points $s, s' \in S$ there exists an isometry U such that: $U(s) = s'$ and $U(S) = S$.*

A finite geometrically uniform signal set S is called a *uniform constellation*, and an infinite signal set S is called a *regular array.*

Definition 2.5. *The* ***generator group*** *$U(S)$ of S is the least subgroup of $\Gamma(S)$ which generates S.*

Theorem 2.1. *The Cartesian product of geometrically uniform signal sets is a geometrically uniform signal set.*

2.2 Projective Spaces and Subspace Codes

Since the vector space of dimension m over a finite field $\mathbb{F}_q$, denoted by $\mathbb{F}_q^m$, is isomorphic to $\mathbb{F}_{q^m}$, we present next some important definitions. For further details, we refer the reader to [1].

Definition 2.6. *The* ***projective space*** *consists of the set of all the vector subspaces of $\mathbb{F}_q^m$ and it is denoted by $\mathbb{P}(\mathbb{F}_q^m)$. Furthermore, the set of all the subspaces with a given fixed dimension k is called* ***Grassmannian*** *and it is denoted by $\mathcal{G}(\mathbb{F}_q^m, k)$.*

Observation 2.2. *Note that:*

$$\mathbb{P}(\mathbb{F}_q^m) = \bigcup_{k=0}^{m} \mathcal{G}(\mathbb{F}_q^m, k).$$

Definition 2.7. *A* ***subspace code*** *$\mathcal{C}$ is a nonempty set of $\mathbb{P}(\mathbb{F}_q^m)$. In the case the subspace code belongs to a Grassmannian of order k, $\mathcal{G}(\mathbb{F}_q^m, k) = \{V \in \mathbb{P}(\mathbb{F}_q^m) : dimV = k\}$, that is, all of its codewords have the same dimension, this code is called* ***subspace code of constant dimension****. We denote by d the minimum distance of $\mathcal{C}$.*

Definition 2.8. *The* ***subspace distance*** *between U and V is defined as:*

$$d(U,V) = dim(U) + dim(V) - 2dim(U \cap V), \tag{1}$$

where $+$ and $\cap$ denote, respectively, the sum and the intersection of subspaces.

Definition 2.9. *The* ***cardinality*** *of $\mathcal{C}$ is given by $\mid \mathcal{C} \mid = M$ and the* ***rate of the code*** *is defined as $R(\mathcal{C}) = \frac{log|\mathcal{C}|}{m}$ or $R(\mathcal{C}) = \frac{logM}{m}$ measured as unity of information per subspace channel use.*

Definition 2.10. *The* ***minimum distance*** *of* $\mathcal{C}$ *is defined as* $d = d(\mathcal{C}) = min\{d(U,V),\ U,\ V \in \mathcal{C},\ U \neq V\}$.

Definition 2.11. *The* ***parameters*** *of the subspace code* $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)$*, are denoted by* (m, M, d)*, where* m *is the dimension of the projective space,* M *is the cardinality, and* d *is the minimum distance. If* $\mathcal{C}$ *belongs to a Grassmannian of dimension* k*, the corresponding parameters are* (m, M, d, k).

Example 2.1. *Let* $\mathbb{F}_2^3$ *be a vector space. An interesting example of a code in a Grassmannian is the simplex code* $\mathcal{C}_2 = \{S_1, S_2, S_3\}$ *with parameters* $(n, M, d, k) = (3, 3, 2, 2)$*, whose codewords, or the vector subspaces, are* $S_1 = \{000, 011, 100, 111\}, S_2 = \{000, 010, 101, 111\}, S_3 = \{000, 001, 110, 111\}$.

2.3 Extended projective subspaces and n-shot subspace codes

Next, we present the main definitions and concepts of n-shot subspace codes, where the objective is to make use of the subspace channel several times, by encoding the information to be transmitted not only in a unique subspace, as in the 1-shot case, but as a sequence of subspaces.

Definition 2.12. *The* ***n-th extension*** *of the projective space* $\mathbb{P}(\mathbb{F}_q^m)$ *is denoted by* $\mathbb{P}(\mathbb{F}_q^m)^n$*, that is, the* n*-th Cartesian product of the projective space. In this way, the elements of* $\mathbb{P}(\mathbb{F}_q^m)^n$ *are* t*-tuples having as components subspaces of the original projective space* $\mathbb{P}(\mathbb{F}_q^m)$.

Definition 2.13. *The* ***extended subspace distance*** *between two elements* $\boldsymbol{U} = (U_1, U_2, ..., U_n)$ *and* $\boldsymbol{V} = (V_1, V_2, ..., V_n)$ *of the extended projective space* $\mathbb{P}(\mathbb{F}_q^m)^n$ *is defined as:*

$$d(\boldsymbol{U}, \boldsymbol{V}) = \sum_{i=1}^{n} d(U_i, V_i), \tag{2}$$

where $d(U_i, V_i) = dim(U_i) + dim(V_i) - 2dim(U_i \cap V_i)$ *for* $i \in \{1, 2, ..., n\}$*. Hence,* $1 \leq d(\boldsymbol{U}, \boldsymbol{V}) \leq m.n$.

Theorem 2.2. $(\mathbb{P}(\mathbb{F}_q^m)^n, d)$ *is a metric space.*

Definition 2.14. *A* ***subspace block code*** *is a nonempty subset* $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ *which is also called an* ***n-shot subspace code****.*

Observation 2.3. *The cardinality, the rate, and the minimum distance of* $\boldsymbol{\mathcal{C}}$ *are defined as usual.*

Definition 2.15. *The* ***parameters*** *of a code* $\boldsymbol{\mathcal{C}} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ *are denoted by* $(m.n, M^n, d)$*, where* $m.n$ *is the dimension of the projective subspace,* M^n *is the cardinality of the code, and* d *is the minimum distance. If* $\boldsymbol{\mathcal{C}}$ *belongs to a Grassmannian of dimension* $k.n$ *the parameters of the code are* $(m.n, M^n, d, k.n)$.

Example 2.2. *Consider the projective space* $\mathbb{P}(\mathbb{F}_2^2) = \{O, S_1, S_2, S_3, W\}$. *A 2-shot subspace code over* $\mathbb{P}(\mathbb{F}_2^2) \times \mathbb{P}(\mathbb{F}_2^2)$ *is:*

$$\mathcal{C} = \{S_1S_1, S_1S_2, S_1S_3, S_2S_1, S_2S_2, S_2S_3, S_3S_1, S_3S_2, S_3S_3\},$$

where $S_1 = \{00, 01\}, S_2 = \{00, 10\}, S_3 = \{00, 11\}$. *Observe that the minimum distance of the code is* $d = 2$. *Thus,* $\mathcal{C}$ *is a 2-shot subspace code.*

3 Geometrically Uniform Subspace Codes

In this section we present the definition of GU subspace codes and GU n-shot subspace codes, as well as a construction of the later code, that is, given a symmetry group the elements of this group act transitively on $\boldsymbol{\mathcal{C}}$.

Definition 3.1. *An isometry* T *of the metric space* $(\mathbb{P}(\mathbb{F}_q^m), d)$ *is a* ***transformation*** $T : \mathbb{P}(\mathbb{F}_q^m) \to \mathbb{P}(\mathbb{F}_q^m)$ *preserving the subspace distance* d, *that is,* $d(T(U), T(V)) = d(U, V)$, *for every* $U, V \in \mathbb{P}(\mathbb{F}_q^m)$.

Definition 3.2. *A* ***subspace code*** $\mathcal{C}$ ***is geometrically uniform*** *if given any two subspaces* $U, V \in \mathcal{C}$ *there exists an isometry* I *such that:* $I(U) = V$ *and* $I(\mathcal{C}) = \mathcal{C}$.

Lemma 3.1. *[5] The transformation* $T_{ij} : \mathcal{C} \subseteq \mathbb{P}(\mathbb{F}_q^m) \to \mathcal{C} \subseteq \mathbb{P}(\mathbb{F}_q^m)$ *defined as:* $T_{ij}(U_i) = U_j$; $T_{ji}(U_j) = U_i$; *and* $T_{ij}(U_k) = U_k$, *where* $k \neq i, j$, *is an isometry for any* $i, j \in \{1, ..., n\}$.

Lemma 3.2. *[5] Code* $\mathcal{C}$ *is a geometrically uniform subspace code under the isometry defined previously.*

Definition 3.3. *An* ***n-shot subspace code*** $\boldsymbol{\mathcal{C}}$ ***is geometrically uniform*** *if given any two vector subspaces* $\boldsymbol{U}, \boldsymbol{V} \in \boldsymbol{\mathcal{C}}$ *there exists an isometry* I *such that:* $I(\boldsymbol{U}) = \boldsymbol{V}$, *and* $I(\boldsymbol{\mathcal{C}}) = \boldsymbol{\mathcal{C}}$.

Lemma 3.3. *The transformation* $T_{ij} : \boldsymbol{\mathcal{C}} = \mathcal{C} \times \mathcal{C} \times ... \times \mathcal{C} \subseteq \mathbb{P}(\mathbb{F}_q^m)^n \to \boldsymbol{\mathcal{C}} = \mathcal{C} \times \mathcal{C} \times ... \times \mathcal{C} \subseteq \mathbb{P}(\mathbb{F}_q^m)^n$ *defined as:* $T_{ij}(\boldsymbol{U}_i) = \boldsymbol{U}_j$; $T_{ji}(\boldsymbol{U}_j) = \boldsymbol{U}_i$; *and* $T_{ij}(\boldsymbol{U}_k) = \boldsymbol{U}_k$, *where* $k \neq i, j$, *is an isometry for every* $i, j \in \{1, ..., n\}$.

Lemma 3.4. *Code* $\boldsymbol{\mathcal{C}}$ *is an* n*-shot geometrically uniform subspace code under the isometry defined previously.*

Definition 3.4. *If* G *is an Abelian* p*-group for some prime* p, *then* G *is also called a* ***p-primary group****.*

Theorem 3.1. *[**Primary Decomposition**][7] Every finite Abelian group* G *is a direct sum of* p*-primary groups.*

Theorem 3.2. *[**Basis Theorem**][7] Every finite Abelian group* G *is a direct sum of cyclic groups.*

Example 3.1. *Consider the projective subspace* $\mathbb{P}(\mathbb{F}_2^3)$. *Code* $\mathcal{C}_2^{(1)} = \{S_1, S_2, S_3\}$, *where* $S_1 = \{000, 100, 010, 110\}$, $S_2 = \{000, 010, 001, 011\}$ *and* $S_3 = \{000, 001, 100, 101\}$ *is geometrically uniform. In fact:*

Consider the matrix $P_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ *generating* S_1, *the matrix* $P_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ *generating* S_2 *and the matrix* $P_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ *generating* S_3.

There exists an Abelian subgroup $Q_1 = \{\sigma_0 = (123); \sigma_1 = (312); \sigma_2 = (231)\}$, *where* $\sigma_0 = Q_1^{(1)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \sigma_1 = Q_2^{(1)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \sigma_2 = Q_3^{(1)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, *which in this case is a cyclic subgroup of the permutation group of order 3, such that:* $P_i + Q_1^{(1)} = P_i$; $P_{(i+1)mod\ 3}Q_2^{(1)} = P_{(i+1)mod\ 3}$; *and* $P_{(i+2)mod\ 3}Q_3^{(1)} = P_{(i+2)mod\ 3}$, *for any* $i \in \{0, 1, 2\}$. *Therefore,* $\mathcal{C}_2^{(1)}$ *is a 1-shot geometrically uniform subspace code with parameters* $(m, M, d, k) = (3, 3, 2, 2)$.

Extending code $\mathcal{C}_2^{(1)}$ for the 2-shot case, we have:

$\boldsymbol{\mathcal{C}_2^{(2)}} = \mathcal{C}_2^{(1)} \times \mathcal{C}_2^{(1)} = \{S_1S_1, S_1S_2, S_1S_3, S_2S_1, S_2S_2, S_2S_3, S_3S_1, S_3S_2, S_3S_3\}$
where:
$S_1S_1 = \langle 000100, 000010, 100000, 010000\rangle$, $S_1S_2 = \langle 000010, 000001, 100000, 010000\rangle$
$S_1S_3 = \langle 000001, 000100, 100000, 010000\rangle$, $S_2S_1 = \langle 000100, 000010, 010000, 001000\rangle$
$S_2S_2 = \langle 000010, 000001, 010000, 001000\rangle$, $S_2S_3 = \langle 000001, 000100, 010000, 001000\rangle$
$S_3S_1 = \langle 000100, 000010, 001000, 100000\rangle$, $S_3S_2 = \langle 000010, 000001, 001000, 100000\rangle$
$S_3S_3 = \langle 000001, 000100, 001000, 100000\rangle$.

Let $\langle e_1, e_2, ..., e_k\rangle$ denote the canonical generators of the subspace. The matrices $P_0, P_1, ..., P_8$ consist of the generators of the row spaces of the corresponding subspaces. Hence, the Abelian subgroup $Q_2 = \{Q_1^{(2)}, Q_2^{(2)}, Q_3^{(2)}, Q_4^{(2)}, Q_5^{(2)}, Q_6^{(2)}, Q_7^{(2)}, Q_8^{(2)}, Q_9^{(2)}\}$, where each element is a 6×6 matrix, is such that:
$Q_1^{(2)} = Q_1^{(1)} \times Q_1^{(1)} \equiv Q_1^{(1)} \oplus Q_1^{(1)}; Q_2^{(2)} = Q_1^{(1)} \times Q_2^{(1)} \equiv Q_1^{(1)} \oplus Q_2^{(1)}$,
$Q_3^{(2)} = Q_1^{(1)} \times Q_3^{(1)} \equiv Q_1^{(1)} \oplus Q_3^{(1)}; Q_4^{(2)} = Q_2^{(1)} \times Q_1^{(1)} \equiv Q_2^{(1)} \oplus Q_1^{(1)}$,
$Q_5^{(2)} = Q_2^{(1)} \times Q_2^{(1)} \equiv Q_2^{(1)} \oplus Q_2^{(1)}; Q_6^{(2)} = Q_2^{(1)} \times Q_3^{(1)} \equiv Q_2^{(1)} \oplus Q_3^{(1)}$,
$Q_7^{(2)} = Q_3^{(1)} \times Q_1^{(1)} \equiv Q_3^{(1)} \oplus Q_1^{(1)}; Q_8^{(2)} = Q_3^{(1)} \times Q_2^{(1)} \equiv Q_3^{(1)} \oplus Q_2^{(1)}$,
$Q_9^{(2)} = Q_3^{(1)} \times Q_3^{(1)} \equiv Q_3^{(1)} \oplus Q_3^{(1)}$. Whose group elements of Q_2 act transitively on the elements of the code $\boldsymbol{\mathcal{C}_2^{(2)}}$, in the following way: $P_iQ_1^{(2)} = P_i$; $P_{(i+1)mod\ 9}Q_2^{(2)} = P_{(i+1)mod\ 9}$; $P_{(i+2)mod\ 9}Q_3^{(2)} = P_{(i+2)mod\ 9}$; $P_{(i+3)mod\ 9}Q_4^{(2)} = P_{(i+3)mod\ 9}$; $P_{(i+4)mod\ 9}Q_5^{(2)} = P_{(i+4)mod\ 9}$; $P_{(i+5)mod\ 9}Q_6^{(2)} = P_{(i+5)mod\ 9}$;

$P_{(i+6)mod\ 9}Q_7^{(2)} = P_{(i+6)mod\ 9}$; $P_{(i+7)mod\ 9}Q_8^{(2)} = P_{(i+7)mod\ 9}$; $P_{(i+8)mod\ 9}Q_9^{(2)} = P_{(i+1)mod\ 9}$, for any $i \in \{0,1,2,3,4,5,6,7,8\}$. Therefore, $\boldsymbol{\mathcal{C}_2^{(2)}}$ is a 2-shot geometrically uniform subspace code with parameters $(m.n, M^n, d, k.n) = (6, 9, 2, 4)$.

Result: Let $\mathcal{C} = \{S_1, S_2, ..., S_M\}$ be a 1-shot geometrically uniform subspace code with parameters (m, M, d, k) for a convenient projective space $\mathbb{P}(\mathbb{F}_2^m)$. There exists an Abelian subgroup $Q_1 = \left\{Q_1^{(1)}, Q_2^{(1)}, ..., Q_M^{(1)}\right\}$ such that the elements of Q_1 act transitively on the subspaces of $\mathcal{C}$. The n-th extension of $\mathcal{C}$ is the code $\boldsymbol{\mathcal{C}} = \mathcal{C} \times \mathcal{C} \times .... \times \mathcal{C}$ for the n-th extension of the projective space, that is, $\boldsymbol{\mathcal{C}}$ is a subspace code in $\mathbb{P}(\mathbb{F}_q^m)^n$ which is geometrically uniform with parameters $(m.n, M^n, d, k.n)$, equivalently, there exists an Abelian subgroup $Q_n = \left\{Q_1^{(n)}, Q_2^{(n)}, ..., Q_{M^n}^{(n)}\right\}$, where each $Q_i^{(n)}$ for $i \in \{1, 2, ..., M^n\}$ is the direct sum of the combination of the elements of Q_1. Thus, $\boldsymbol{\mathcal{C}}$ is an n-shot geometrically uniform subspace code.

4 Conclusion

We have established in this paper the main concepts of geometrically uniform subspace codes and a new class of n-shot geometrically uniform subspace codes which have interesting algebraic and geometric properties from both the mathematical and communication theory points of view. Furthermore, the importance of these codes is related to the existing efficient decoding algorithms.

References

[1] T. Etzion, A. Vardy, Error Correcting Codes in Projective Space, in Proc. of the 2008 IEEE Intl Symp. Inform. Theory - ISIT-08, pp. 871-875, Toronto, Canada, Jul. 2008.

[2] G. D. Forney Jr., Geometrically Uniform Codes, IEEE Trans. on Inform. Theory, vol. 37, n. 5, pp. 1241-1260, Sep., 1991.

[3] A. Khaleghi, D. Silva, F.R. Kschischang, Subspace Codes, Lecture Notes in Computer Science, vol. 5921, pp. 1-21, 2009.

[4] H. Lazari, A Contribution to the Theory of Geometrically Uniform Hyperbolic Codes, PhD Dissertation, FEEC-UNICAMP, Brasil, 2000 (in Portuguese).

[5] G.A.Miyamoto, Geometrically Uniform Subspace Codes, MS Thesis, FEEC-UNICAMP, Mar. 2015 (in Portuguese).

[6] R. Nobrega, B. Uchoa-Filho, Multishot Codes for Network Coding: Bounds and a Multilevel Construction, in Proc. of the 2009 IEEE Intl Symp. on Information Theory - ISIT-09, Seoul, South Korea, Jun. 2009.

[7] J.J.Rotman, An Introduction to the Theory of Groups, 4th edition, Springer Verlag, New York, United States of America, 1999.