21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

On the Cardinality and Distance of Cyclic Orbit Codes based on Stabilizer Subfields

Heide Gluesing-Luerssen[1], Katherine Morrison[2], Carolyn Troha[1]

***Abstract*— Cyclic orbit codes are constant dimension subspace codes that arise as the orbit of a cyclic subgroup of the general linear group acting on subspaces in the given ambient space. With the aid of the largest subfield over which the given subspace is a vector space, the cardinality of the orbit code can be determined, and estimates for its distance can be found. This subfield is closely related to the stabilizer of the generating subspace.**

I. Introduction

Subspace codes have gained considerable attention during the last decade due to their crucial role in random network coding, see for instance the articles [4], [5] and the references therein. Specific subspace codes with large distance were found by computer search in, for instance, [2], [6], and particular constructions were studied in [1], [7], [8]. There is a close link between the subspace codes in [2], [6] and in [7], [8]: in the second set of papers the subspace codes are orbits with respect to a particular cyclic group, whereas in the first set of papers the codes are invariant under the same group, and thus are unions of such orbits.

In this note we will provide further insight into the class of cyclic orbit codes. The results in the aforementioned papers show a promising potential of these codes due to their specific algebraic structure.

Throughout, let $\mathbb{F} := \mathbb{F}_q$ be a finite field of size q. Recall that a *subspace code* over $\mathbb{F}$ is simply a collection of subspaces of $\mathbb{F}^n$. The code is called a *constant dimension code* if all its subspaces have the same dimension. The *subspace distance* of a subspace code $\mathcal{C}$ is defined as $\mathrm{d_S}(\mathcal{C}) := \min\{\mathrm{d_S}(\mathcal{V},\mathcal{W}) \mid \mathcal{V}, \mathcal{W} \in \mathcal{C}, \mathcal{V} \neq \mathcal{W}\}$, where the distance between two subspaces is

$$\mathrm{d_S}(\mathcal{V},\mathcal{W}) := \dim \mathcal{V} + \dim \mathcal{W} - 2\dim(\mathcal{V} \cap \mathcal{W}).$$

II. Cyclic Orbit Codes

Throughout this work, we will make use of the fact that $\mathbb{F}^n$ is isomorphic to the $\mathbb{F}$-vector space $\mathbb{F}_{q^n}$. Thus, we may consider subspace codes as collections of subspaces in $\mathbb{F}_{q^n}$ and at the same time utilize the field structure of $\mathbb{F}_{q^n}$.

We fix a primitive element α of $\mathbb{F}_{q^n}$, thus

$$\mathbb{F}_{q^n}^* := \mathbb{F}_{q^n} \backslash \{0\} = \langle \alpha \rangle,$$

where the latter denotes the cyclic group generated by α. The codes under consideration are derived from the natural action of the group $\langle \alpha \rangle$ on $\mathbb{F}_{q^n}$. This action induces an action on the set of subspaces of $\mathbb{F}_{q^n}$, and thus gives rise to the following type of constant dimension codes. These codes were introduced in a slightly different form in [7], [8].

Definition 2.1: Let $\mathcal{U}$ be a k-dimensional subspace of the $\mathbb{F}$-vector space $\mathbb{F}_{q^n}$. The *cyclic orbit code* generated by $\mathcal{U}$ is defined as the set

$$\mathrm{Orb}(\mathcal{U}) := \{\mathcal{U}\alpha^i \mid i = 0, 1, \ldots, q^n - 2\}.$$

Obviously, $\mathcal{C} := \mathrm{Orb}(\mathcal{U})$ is a constant dimension subspace code. Let us briefly describe the translation of this setting into subspace codes in $\mathbb{F}^n$. Using the basis $1, \alpha, \ldots, \alpha^{n-1}$ for the coordinate map between $\mathbb{F}_{q^n}$ and $\mathbb{F}^n$ it is clear that this map turns $\mathrm{Orb}(\mathcal{U})$ into an orbit of the cyclic subgroup generated by the companion matrix of α under the natural action on the subspaces of $\mathbb{F}^n$. This is the setting primarily studied in [7], [8]. On the other hand, in [2, p. 1170], the authors introduce *cyclic* subspace codes in $\mathbb{F}_{q^n}$. In our terminology, these codes are unions of orbit codes $\bigcup_{t=1}^{T} \mathrm{Orb}(\mathcal{U}_t)$. With the aid of a computer search, they are able to find interesting cyclic codes that come close to known bounds for subspace codes. Even larger and better unions of this type have been found in [6, Sec. 5].

We close this section with the following simple fact. The dual of a subspace code $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{\mathcal{V}^\perp \mid \mathcal{V} \in \mathcal{C}\}$. It is easy to see that the dual of an orbit code is, up to linear isometry, an orbit code again; see also [8, Thm. 18]. Since $\mathrm{d_S}(\mathcal{C}) = \mathrm{d_S}(\mathcal{C}^\perp)$, see [2, Lem. 13], we may and will restrict ourselves to cyclic orbit codes generated by subspaces of dimension at most $n/2$.

III. Stabilizer Group and Cardinality of Cyclic Orbit Codes

Fix a k-dimensional subspace $\mathcal{U}$ of $\mathbb{F}_{q^n}$. Without loss of generality we may assume that $1 \in \mathcal{U}$.

Consider the orbit code $\mathrm{Orb}(\mathcal{U})$ as in Definition 2.1. The stabilizer of $\mathcal{U}$ under the group action induced by $\langle \alpha \rangle = \mathbb{F}_{q^n}^*$ is $\mathrm{Stab}(\mathcal{U}) := \{\gamma \in \mathbb{F}_{q^n}^* \mid \mathcal{U}\gamma = \mathcal{U}\} = \{\gamma \in \mathbb{F}_{q^n}^* \mid \mathcal{U}\gamma \subseteq \mathcal{U}\}$. Let $N \in \mathbb{N}$ be the minimal integer such that $\mathrm{Stab}(\mathcal{U}) = \langle \alpha^N \rangle$. Then N is a divisor of $q^n - 1$ and

$$\left.\begin{aligned} &|\mathrm{Stab}(\mathcal{U})| = \tfrac{q^n-1}{N}, \\ &\mathrm{Orb}(\mathcal{U}) = \{\mathcal{U}\alpha^i \mid i = 0, \ldots, N-1\}, \\ &|\mathrm{Orb}(\mathcal{U})| = N. \end{aligned}\right\} \qquad (1)$$

*HGL was partially supported by the National Science Foundation Grant DMS-1210061.

** This conference note is based on the preprint [3].

[1]HGL and CT are with the Department of Mathematics, University of Kentucky, Lexington KY 40506-0027, USA; {heide.gl, carolyn.troha}@uky.edu

[2]KM is with the School of Mathematical Sciences, University of Northern Colorado, Greeley, CO 80639, USA; Katherine.Morrison@unco.edu.

ISBN: 978-90-367-6321-9

Definition 3.1: Let $\mathrm{Stab}^+(\mathcal{U})$ be the smallest subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}$ and the group $\mathrm{Stab}(\mathcal{U})$.

It is clear that $\mathrm{Stab}^+(\mathcal{U})$ is the field extension $\mathbb{F}[\alpha^N]$. In fact one can show

Proposition 3.2: $\mathrm{Stab}^+(\mathcal{U}) = \mathrm{Stab}(\mathcal{U}) \cup \{0\}$ and $\mathrm{Stab}^+(\mathcal{U})$ is contained in $\mathcal{U}$. Moreover, $\mathcal{U}$ is a vector space over $\mathrm{Stab}^+(\mathcal{U})$ with scalar multiplication being the multiplication of the field $\mathbb{F}_{q^n}$.

In the case where n is prime, the only proper subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}$ is $\mathbb{F}$ itself.

Corollary 3.3: If n is prime, then for every proper subspace $\mathcal{U} \subset \mathbb{F}_{q^n}$ we have $\mathrm{Stab}(\mathcal{U}) = \mathbb{F}^*$ and $|\mathrm{Orb}(\mathcal{U})| = \frac{q^n-1}{q-1}$.

The following terminology will be convenient as the concept arises repeatedly in this work.

Definition 3.4: A subfield $\mathbb{F}_{q^r}$ of $\mathbb{F}_{q^n}$ is called a *friend* of $\mathcal{U}$ if $\mathcal{U}$ is an $\mathbb{F}_{q^r}$-vector space with scalar multiplication being the multiplication in the field $\mathbb{F}_{q^n}$. The largest friend of $\mathcal{U}$ (with respect to cardinality) is called the *best friend* of $\mathcal{U}$.

Note that since $\mathcal{U}$ is a subspace of the $\mathbb{F}$-vector space $\mathbb{F}_{q^n}$, the field $\mathbb{F}$ is a friend of $\mathcal{U}$, and thus $\mathcal{U}$ also has a best friend. Furthermore, since $1 \in \mathcal{U}$, the best friend of $\mathcal{U}$ is contained in $\mathcal{U}$.

Proposition 3.5: The subfield $\mathrm{Stab}^+(\mathcal{U})$ is the best friend of $\mathcal{U}$. Furthermore, any friend of $\mathcal{U}$ is contained in the best friend.

Now we may rewrite the identities in (1) as follows. This result facilitates the design of orbit codes with a prescribed cardinality.

Theorem 3.6: Let $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$. Then $|\mathrm{Orb}(\mathcal{U})| = \frac{q^n-1}{q^r-1}$. As a consequence, $|\mathrm{Orb}(\mathcal{U})| = \frac{q^n-1}{q^k-1}$ if and only if $\mathcal{U} = \mathbb{F}_{q^k}$. Moreover, $\mathrm{d_S}\big(\mathrm{Orb}(\mathbb{F}_{q^k})\big) = 2k$.

The last part of this result recovers known facts about spread codes. Recall that a subspace code $\mathcal{C}$ is called a *spread* of $\mathbb{F}_{q^n}$ if $\bigcup_{\mathcal{V}\in\mathcal{C}} \mathcal{V} = \mathbb{F}_{q^n}$ and $\mathcal{V} \cap \mathcal{W} = \{0\}$ for all distinct $\mathcal{V}, \mathcal{W} \in \mathcal{C}$. Thus, $\mathrm{Orb}(\mathbb{F}_{q^k})$ is a k-dimensional spread, which can also be found in [7, Thm. 11, Cor. 12]. The first part of Theorem 3.6 shows that among all cyclic orbit codes generated by a k-dimensional subspace, the spread code has the least cardinality.

IV. The Subspace Distance of Cyclic Orbit Codes

As before, let $\mathcal{U}$ be a k-dimensional subspace of $\mathbb{F}_{q^n}$ such that $1 \in \mathcal{U}$ and where $k \leq n/2$. Furthermore, let $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$, and define $t := \frac{k}{r} = \dim_{\mathbb{F}_{q^r}} \mathcal{U}$.

The following lemma shows that the subspace distance is a multiple of $2r$. This is due to the simple fact that the intersection of any two subspaces in $\mathrm{Orb}(\mathcal{U})$ is a vector space over $\mathbb{F}_{q^r}$.

Lemma 4.1: Define $s := \max_{1\leq j<N} \dim_{\mathbb{F}_{q^r}}(\mathcal{U} \cap \mathcal{U}\alpha^j)$. Then

$$\mathrm{d_S}(\mathrm{Orb}(\mathcal{U})) = 2(k - sr) = 2(t - s)r. \tag{2}$$

As a consequence, $2r \leq \mathrm{d_S}\big(\mathrm{Orb}(\mathcal{U})\big) \leq 2k$.

The upper bound $\mathrm{d_S}\big(\mathrm{Orb}(\mathcal{U})\big) \leq 2k$ is true for all constant dimension codes of dimension k; this follows immediately from the definition of the subspace distance. The lemma yields the equivalences

$$\mathrm{d_S}(\mathrm{Orb}(\mathcal{U})) = 2k \iff r = k \iff \mathcal{U} = \mathbb{F}_{q^k}.$$

If any of this is true, $\mathrm{Orb}(\mathcal{U})$ is a spread code. Recall from Theorem 3.6 that these codes have the smallest cardinality among all k-dimensional orbit codes.

Comparing the lower bound $2r$ with Theorem 3.6 we observe the usual trade-off between the cardinality of a code and its (potential) distance: the larger the best friend, the smaller the code, but the better the lower bound for the distance.

The next result shows that the worst distance, namely $\mathrm{d_S}(\mathrm{Orb}(\mathcal{U})) = 2r$, is attained by the following subspaces.

Proposition 4.2: Suppose $\mathcal{U}$ is of the form

$$\mathcal{U} = \bigoplus_{i=0}^{t-1} \alpha^{li}\mathbb{F}_{q^r} \text{ for some } 1 \leq l < \frac{q^n-1}{q^r-1},$$

where $\mathbb{F}_{q^r}$ is the best friend of $\mathcal{U}$. Then $\mathrm{d_S}(\mathrm{Orb}(\mathcal{U})) = 2r$.

Observe that we added the requirement that $\mathbb{F}_{q^r}$ be the best friend of $\mathcal{U}$ because this does not follow from the form of $\mathcal{U}$. Indeed, $\mathcal{U} = \bigoplus_{i=0}^{t-1} \alpha^{li}\mathbb{F}_{q^r}$ only implies that $\mathbb{F}_{q^r}$ is a friend of $\mathcal{U}$, but it may not be the best friend. For instance, in $\mathbb{F}_{2^6}$ with primitive element α we have $\mathbb{F}_{2^2} = \mathbb{F}_2 \oplus \alpha^{21}\mathbb{F}_2$, hence the best friend is $\mathbb{F}_{2^2}$. The following result shows that this is essentially the only case where $\mathbb{F}_{q^r}$ is not the best friend.

Theorem 4.3: Let $\mathcal{U} = \bigoplus_{i=0}^{t-1} \alpha^{il}\mathbb{F}_{q^r}$ for some l and where $t > 1$. Then the minimal polynomial of α^l over $\mathbb{F}_{q^r}$ satisfies $\deg(\mathrm{minpoly}(\alpha^l, \mathbb{F}_{q^r})) \geq t$. Furthermore,

$$\begin{aligned} \mathcal{U} = \mathbb{F}_{q^{rt}} &\iff \deg(\mathrm{minpoly}(\alpha^l, \mathbb{F}_{q^r})) = t \\ &\iff \alpha^l\mathcal{U} = \mathcal{U} \\ &\iff \mathbb{F}_{q^r} \text{ is not the best friend of } \mathcal{U}. \end{aligned}$$

In other words, $\mathbb{F}_{q^r}$ is the best friend of $\mathcal{U}$ if and only if $\mathcal{U}$ is not a field.

Of course, there are also subspaces that are not of the form as in Lemma 4.2 that generate orbit codes with distance as low as $2r$.

Let us now return to the case where the distance is large. According to Lemma 4.1 the best distance a non-spread orbit code may achieve is $2(k-r)$. Many examples of such codes can be found. For instance, the cyclic orbit codes that form the building blocks of the codes in [2, p. 1170] are optimal among all non-spread orbit codes. Also, most of the cyclic codes found in [6, Sec. 5] are of this type. Some of these codes even beat the best codes that were known previously.

Example 4.4: Suppose $\dim_{\mathbb{F}_{q^r}}(\mathcal{U}) = t = 2$, hence $k = 2r$. In this case $2r = 2(k-r)$ and Lemma 4.1 yields $\mathrm{d_S}(\mathrm{Orb}(\mathcal{U})) = 2(k-r)$. Thus the code is optimal among all non-spread orbit codes.

Unfortunately, beyond this case we are not aware of a general construction that guarantees the distance $2(k-r)$.

V. Future Research

In addition to the previous results, the concept of best friends can be utilized to improve upon a result determining the distance of a cyclic orbit code via certain integer multi-sets presented in [6], [7]. Since this was used in [6] to efficiently search for large unions of orbit codes with good distance, we believe that this direction needs to be further pursued.

More generally, it is left to future research to further explore the potential of cyclic orbit codes and unions thereof. The examples in [2], [6] illustrate their quality with respect to distance properties. In this context, a natural generalization, namely cyclic codes with respect to a proper subgroup of $\mathbb{F}_{q^n}^*$, should be included in the investigation. Finally, it remains to be studied whether the cyclic structure of these codes can be utilized for efficient decoding algorithms.

References

[1] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Trans. Inform. Theory*, IT-55:2909–2919, 2009.

[2] T. Etzion and A. Vardy. Error-correcting codes in projective space. *IEEE Trans. Inform. Theory*, IT-57:1165–1173, 2011.

[3] H. Gluesing-Luerssen, K. Morrison, and C. Troha. Cyclic orbit codes and stabilizer subfields. Preprint 2014. Submitted. arXiv:1403.1218v1 [cs.IT].

[4] A. Khaleghi, D. Silva, and F. R. Kschischang. Subspace codes. In *Proc. 12th IMA Conf. Cryptography Coding*, pages 1–21, Cirencester, U.K., 2009.

[5] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inform. Theory*, IT-54:3579–3591, 2008.

[6] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In J. Calmet, W. Geiselmann, and J. Müller-Quade, editors, *Mathematical Methods in Computer Science*, volume 5393, pages 31–42. Lecture Notes in Computer Science; Springer, Berlin, 2008. arXiv: 0807.3212v1 [cs.IT].

[7] J. Rosenthal and A.-L. Trautmann. A complete characterization of irreducible cyclic orbit codes and their Plücker embedding. *Des. Codes Cryptogr.*, 66:275–289, 2013.

[8] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *IEEE Trans. Inform. Theory*, IT-59:7386–7404, 2013.