Subspace Polynomials and Cyclic Subspace Codes

Eli Ben-Sasson[†] Tuvi Etzion[*] Ariel Gabizon[†] Netanel Raviv[*]

Abstract

Subspace codes have received an increasing interest recently due to their application in error-correction for random network coding. In particular, cyclic subspace codes are possible candidates for large codes with efficient encoding and decoding algorithms. In this paper we consider such cyclic codes and provide constructions of optimal codes for which their codewords do not have full orbits. We further introduce a new way to represent subspace codes by a class of polynomials called subspace polynomials. We present some constructions of such codes which are cyclic and analyze their parameters.

I. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of size q, and let $\mathbb{F}_q^* \triangleq \mathbb{F}_q \setminus \{0\}$. For $n \in \mathbb{N}$ denote by $\mathbb{F}_{q^n}$ the field extension of degree n of $\mathbb{F}_q$ which may be seen as the vector space of dimension n over $\mathbb{F}_q$. By abuse of notation, we will not distinguish between these two concepts. Given a non-negative integer $k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_{q^n}$ forms a *Grassmannian* space (Grassmannian in short) over $\mathbb{F}_q$, which is denoted by $\mathcal{G}_q(n, k)$. The size of $\mathcal{G}_q(n, k)$ is given by the well-known Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$. The set of all subspaces of $\mathbb{F}_{q^n}$ is called the *projective space* of order n over $\mathbb{F}_q$ [9] and is denoted by $\mathcal{P}_q(n)$. The set $\mathcal{P}_q(n)$ is endowed with the metric $d(U, V) = \dim U + \dim V - 2 \dim(U \cap V)$. A subspace code is a collection $\mathbb{C}$ of subspaces from $\mathcal{P}_q(n)$. In this paper we will be mainly interested in *constant dimension* codes (called also Grassmannian codes), that is, $\mathbb{C} \subseteq \mathcal{G}_q(n, k)$ for some $k \leq n$.

Subspace codes and constant dimension codes have attracted a lot of research in the last eight years. The motivation was given in [13], where it was shown how subspace codes may be used in random network coding for correction of errors and erasures. This application of subspace codes renewed the interest in a wide variety of problems related to vector spaces [1], [7], [18], [21], particularly in constructions of large codes with error correction capability, efficient encoding algorithms for these codes, as well as efficient decoding algorithms.

In [13] a novel construction of large subspace codes using *linearized polynomials* (a.k.a. *p*-polynomials [19]) is presented. These codes were later shown [20] to be related to optimal rank-metric codes through an operation called *lifting*. These two techniques and some of their variants are the main known tools for constructing subspace codes.

It was previously suggested [5], [9], [14] that *cyclic subspace codes* may present a useful structure that can be applied efficiently for the purpose of coding. For a subspace $V \in \mathcal{G}_q(n, k)$ and $\alpha \in \mathbb{F}_{q^n}^*$ we define the *cyclic shift* of V as $\alpha V \triangleq \{\alpha v \mid v \in V\}$. The set αV is clearly a subspace of the same dimension as V. Two cyclic shifts are called *distinct* is they form two different subspaces. A subspace code $\mathbb{C}$ is called *cyclic* if for every $\alpha \in \mathbb{F}_{q^n}^*$ and every $V \in \mathbb{C}$ we have $\alpha V \in \mathbb{C}$.

In [9], [14] several examples of optimal cyclic subspace codes with small dimension were found. In [5] an optimal code which also forms a q-analog of Steiner system was presented. This code has an automorphism group which is generated by a cyclic shift and the Frobenius mapping (known together also as a normalizer of a Singer subgroup [5],[12, pp. 187-188]). These codes raised the plausible conjecture that large cyclic codes may be constructed in any dimension. However, the current approaches for construction of subspace codes fall short with handling cyclic codes. In this paper we aim at establishing new general techniques for constructions of cyclic codes.

In [22] a thorough algebraic analysis of the structure of cyclic orbit codes is given. One class of such codes is the cyclic codes. However, no nontrivial construction is given. In [10] a construction of cyclic codes with degenerated orbit (of size less than $\frac{q^n-1}{q-1}$) is given. This construction produces a subcode of some codes in our work (see Section III-B). Both [10] and [22] raised the following conjecture:

Conjecture 1. *For every positive integers n, k such that $k < n/2$, there exists a cyclic code of size $\frac{q^n-1}{q-1}$ in $\mathcal{G}_q(n, k)$ and minimum distance $2k - 2$.*

Notice that for $k > n/2 + 1$, a minimum distance of $2k - 2$ is clearly not possible. The original conjecture [22] considered $k \leq n/2$. However, an exhaustive search which was used in [10] proved that the conjecture is false for $n = 8, k = 4, q = 2$. When $k < n/2$, it appears that there is enough flexibility that many such codes exist, while for $k = n/2$, such a code might not exist. Its existence depends on the existence of a subspace which forms a structure similar to a difference set [5]. In this paper it is proved that this conjecture is true for a given k and infinitely many values of n, along with several options for explicit constructions (see Theorem 3). In [10], [22] it was also pointed out that it is not known how to construct cyclic codes with multiple orbits. In the sequel we show that our techniques can be useful for this purpose (see Lemma 12 and Construction 1).

One of the tools in our constructions is the so-called subspace polynomials, which are a special case of linearized polynomials. Subspace polynomials form an efficient method of representing subspaces, from which one can directly deduce certain properties of the subspace which are not evident in some other representations. These objects were studied in the past for various purposes, e.g., bounds on list-decoding of Reed-Solomon and rank-metric codes [23], construction of affine dispersers [3], and finding an element of high multiplicative order in a finite field [6].

The rest of this paper is organized as follows. Section II will start with the known definition of subspace polynomials. We continue to analyze properties of the subspaces corresponding to the subspace polynomials, in particular we examine distance properties induced by cyclic and Frobenius shifts of these subspaces. Based on these properties, in Section III we consider constructions of optimal cyclic codes with degenerate orbits, and cyclic codes with full orbits. The main goal in constructing cyclic codes is to obtain as many orbits as possible in the code. This task will be left for future work. In this work we consider first the existence of cyclic codes with one full length orbit and cyclic codes with multiple full length orbits. Conclusions are given in Section IV.

II. SUBSPACES AND THEIR SUBSPACE POLYNOMIALS

For the rest of this paper k and n will be positive integers such that $2 < k < n$, and we denote $[\ell] \triangleq q^\ell$. We begin by defining linearized polynomials and subspace polynomials.

Definition 1. *A linearized polynomial was defined by Ore [19] as follows:*

$$P(x) \triangleq a_k \cdot x^{[k]} + a_{k-1} \cdot x^{[k-1]} + \cdots + a_1 \cdot x^{[1]} + a_0 \cdot x$$

where the coefficients are in the finite field $\mathbb{F}_{q^n}$.

Linearized polynomials have numerous applications in classic coding theory (e.g., [17, Chapter 4]). It is widely known that the roots of any linearized polynomial form a subspace in some extension of $\mathbb{F}_{q^n}$ (seen as a vector space over $\mathbb{F}_q$) and for every $V \in \mathcal{G}_q(k, n)$, the polynomial $\prod_{v \in V}(x - v)$ is a linearized polynomial [17, p. 118]. We will be particulary interested in linearized polynomials that have simple roots with respect to some field $\mathbb{F}_{q^n}$.

Definition 2. *[3], [4], [6], [23] A monic linearized polynomial P with coefficients in $\mathbb{F}_{q^n}$ is called a subspace polynomial with respect to $\mathbb{F}_{q^n}$ if the following equivalent conditions hold:*

1) *P divides $x^{[n]} - x$.*
2) *P splits completely over $\mathbb{F}_{q^n}$ and all its roots have multiplicity 1.*

From now on, we shall omit the notation of $\mathbb{F}_{q^n}$ whenever it is clear from context. The first two lemmas are trivial and well known. The simplicity of the roots of a subspace polynomial (and in particular, the simplicity of 0) gives rise to the following lemma.

Lemma 1. *In any subspace polynomial, the coefficient of x is non-zero. Conversely, every linearized polynomial with non-zero coefficient of x is a subspace polynomial in its splitting field.*

Proof: It is readily verified that 0 is a root of multiplicity 1 if and only if the coefficient of x is non-zero. Therefore, if P is a subspace polynomial, all of his roots are of multiplicity 1 (see Definition 2), including 0. On the other hand, if Q is a linearized polynomial with a non-zero coefficient of x, then by [15, Theorem 3.50, p. 108], all the roots of Q have multiplicity 1. ∎

It also follows from Definition 2 that for a given $V \in \mathcal{G}_q(n, k)$ the polynomial $\prod_{v \in V}(x - v)$ is the unique subspace polynomial whose set of roots is V, which leads to the following lemma.

Lemma 2. *Two subspaces are equal if and only if their corresponding subspace polynomials are equal.*

Lemma 2 allows us to denote by P_V the unique subspace polynomial corresponding to a given subspace V.

Example 1. *Let t be a positive integer such that $t|n$. It is known that $\mathbb{F}_{q^t}$ is a subfield (in particular, a subspace) of $\mathbb{F}_{q^n}$. The subspace polynomial of $\mathbb{F}_{q^t}$ is $P_{\mathbb{F}_{q^t}}(x) = x^{[t]} - x$.*

The connection between linearized polynomials and subspace polynomial is given by the following two claims.

Theorem 1. *[15, Theorem 3.50, p. 108] If P is a linearized polynomial whose splitting field is $\mathbb{F}_{q^n}$, then each root of P in $\mathbb{F}_{q^n}$ has the same multiplicity, which is a non-negative power of q, and the roots form a linear subspace of $\mathbb{F}_{q^n}$.*

Lemma 3. *If $P(x)$ is a linearized polynomial with a leading coefficient* $\alpha \neq 0$ and the splitting field of $P(x)$ is $\mathbb{F}_{q^n}$, then $P(x) = \alpha P_V(x)^{[t]}$ for some subspace V in $\mathbb{F}_{q^n}$ and some $t \in \mathbb{N}$.*

---

*The leading coefficient of a polynomial is the coefficient of the monomial with the highest degree.

Proof: According to Theorem 1, all the roots of P are of the same multiplicity q^t for some $t \in \mathbb{N}$, and these roots form a subspace V of $\mathbb{F}_{q^n}$. Hence,

$$P(x) = \alpha \prod_{v \in V} (x - v)^{[t]} = \alpha \left(\prod_{v \in V} (x - v) \right)^{[t]} = \alpha P_V(x)^{[t]}.$$

■

In the sequel, we show several connections between the coefficients of subspace polynomials and properties of the respective subspaces. One of the main tools in our analysis is the difference between the indices of the two topmost non-zero coefficients:

Definition 3. *For $V \in \mathcal{G}_q(n, k)$ and $P_V(x) = x^{[k]} + \sum_{j=0}^{i} \alpha_j x^{[j]}$, where $\alpha_i \neq 0$, let $\mathrm{gap}(V) \triangleq k - i$.*

As the following lemma illustrates, the gap of two subspace induces a lower bound on their related distance.

Lemma 4. *If $V \in \mathcal{G}_q(n, k_1)$ and $U \in \mathcal{G}_q(n, k_2)$ are two distinct subspaces such that $k_1 \leq k_2$ and*

$$P_V(x) = x^{[k_1]} + \sum_{j=0}^{t} \alpha_j x^{[j]}$$

$$P_U(x) = x^{[k_2]} + \sum_{j=0}^{s} \beta_j x^{[j]},$$

such that $\alpha_t \neq 0$ and $\beta_s \neq 0$, then $\dim(U \cap V) \leq \max(s, t + k_2 - k_1)$.

Proof: According to the properties of $\mathbb{F}_{q^n}$, for all $\alpha, \beta \in \mathbb{F}_{q^n}$ and for all $i \in \mathbb{N}$ we have that $(\alpha + \beta)^{[i]} = \alpha^{[i]} + \beta^{[i]}$, and therefore

$$P_V(x)^{[k_2 - k_1]} = x^{[k_2]} + \sum_{j=0}^{t} \alpha_j^{[k_2 - k_1]} x^{[j + k_2 - k_1]}.$$

Since the polynomials $P_V, P_V^{[k_2 - k_1]}$ have the same set of roots, and since the roots of P_U are simple, it follows that[†] $\gcd(P_V, P_U) = \gcd(P_V^{[k_2 - k_1]}, P_U)$. Hence, if $Q(x) \triangleq P_U(x) - P_V(x)^{[k_2 - k_1]}$ then

$$\begin{aligned} \gcd(P_V, P_U) &= \gcd(P_V^{[k_2 - k_1]}, P_U) \\ &= \gcd(P_V^{[k_2 - k_1]}, P_U(mod\ P_V^{[k_2 - k_1]})) \\ &= \gcd(P_V^{[k_2 - k_1]},\ Q(mod\ P_V^{[k_2 - k_1]})). \end{aligned}$$

Since $\deg Q \leq \max([s], [t + k_2 - k_1])$, it follows that

$$\log_q \deg \gcd(P_V^{[k_2 - k_1]}, Q(mod\ P_V^{[k_2 - k_1]})) \leq \max(s, t + k_2 - k_1),$$

and hence $\dim(U \cap V) \leq \max(s, t + k_2 - k_1)$. ■

A special case of Lemma 4, where the subspaces U and V are of the same dimension k, provides the following useful corollaries.

Corollary 1. *If $U, V \in \mathcal{G}_q(n, k)$ then $\dim(U \cap V) \leq k - \min(\mathrm{gap}(U), \mathrm{gap}(V))$.*

Corollary 2. *If $U, V \in \mathcal{G}_q(n, k)$ then $d(U, V) \geq 2\min(\mathrm{gap}(U), \mathrm{gap}(V))$.*

[†]$\gcd(s, t)$ stands for the greatest common denominator of the elements s, t.

Remark 1. *Corollary 2 is not tight, i.e., there exists subspaces $U, V \in \mathcal{G}_q(n, k)$ where $\mathrm{gap}(V) = gap(U) = 1$ and $d(U, V) = 2k - 2$. For example, let γ be a root of $x^7 + x + 1 = 0$, and use this primitive polynomial to generate $\mathbb{F}_{2^7}$. The following polynomials are subspace polynomials of $U, V \in \mathcal{G}_2(7, 3)$ for which $\mathrm{gap}(U) = \mathrm{gap}(V) = 1$ and $d(U, V) = 2 \cdot 3 - 2 \cdot 1 = 4$. In particular, U and V are cyclic shifts of each other.*

$$
\begin{aligned}
P_U(x) &= x^{[3]} + x^{[2]} + (\gamma^6 + \gamma^4 + \gamma^3 + \gamma + 1)x^{[1]} + (\gamma^3 + \gamma^2 + \gamma + 1)x \\
P_V(x) &= x^{[3]} + (\gamma^2 + 1)x^{[2]} + (\gamma^6 + \gamma^4 + \gamma + 1)x^{[1]} + (\gamma^5 + \gamma^4 + \gamma)x
\end{aligned}
$$

Aside from cyclic shifts we will also use the well known *Frobenius mapping F^i* as a method to increase the size of the codes. For an element $\alpha \in \mathbb{F}_{q^n}$ and $i \in \{0, \ldots, n-1\}$, the $\mathbb{F}_q$-mapping F^i is defined as $F^i(\alpha) = \alpha^{[i]}$ (see [15, p. 75]). For a subspace V and $i \in \{0, \ldots, n-1\}$ the ith *Frobenius shift* of V is defined as $F^i(V) \triangleq \{v^{[i]} \mid v \in V\}$. Since the function F^i is an automorphism, it follows that the set $F^i(V)$ is a subspace of the same dimension as V. We now characterize the subspace polynomials of the subspaces resulting from these mappings.

Lemma 5. *If $V \in \mathcal{G}_q(n, k)$ and $\alpha \in \mathbb{F}_{q^n}^*$ then $P_{\alpha V}(x) = \alpha^{[k]} \cdot P_V(\alpha^{-1}x)$. That is, if $P_V(x) = x^{[k]} + \sum_{j=0}^{i} \alpha_j x^{[j]}$ then $P_{\alpha V}(x) = x^{[k]} + \sum_{j=0}^{i} \alpha^{[k]-[j]} \alpha_j x^{[j]}$.*

Proof: By definition,

$$
\begin{aligned}
P_{\alpha V}(x) &= \prod_{u \in \alpha V} (x - u) \\
&= \prod_{v \in V} (x - \alpha v) \\
&= \alpha^{[k]} \prod_{v \in V} (\alpha^{-1}x - v) \\
&= \alpha^{[k]} \cdot P_V(\alpha^{-1}x) \\
&= x^{[k]} + \sum_{j=0}^{i} \alpha^{[k]-[j]} \alpha_j x^{[j]}.
\end{aligned}
$$

∎

Lemma 6. *If $V \in \mathcal{G}_q(n, k)$ and $P_V(x) = x^{[k]} + \sum_{j=0}^{i} \alpha_j x^{[j]}$ then for all $s \in \{0, \ldots, n-1\}$, $P_{F^s(V)}(x) = x^{[k]} + \sum_{j=0}^{i} F^s(\alpha_j)x^{[j]}$.*

Proof: If $s \in \{0, \ldots, n-1\}$ and $u \in F^s(V)$ then $u = F^s(v)$ for some $v \in V$. Since F^s is an automorphism, it follows that

$$
\begin{aligned}
u^{[k]} + \sum_{j=0}^{i} F^s(\alpha_j)u^{[j]} &= F^s(v)^{[k]} + \sum_{j=0}^{i} F^s(\alpha_j)F^s(v)^{[j]} \\
&= F^s(v^{[k]}) + \sum_{j=0}^{i} F^s(\alpha_j v^{[j]}) = F^s\left(v^{[k]} + \sum_{j=0}^{i} \alpha_j v^{[j]}\right) \\
&= F^s(P_V(v)) = F^s\left(\prod_{w \in V}(v - w)\right) = F^s(0) = 0.
\end{aligned}
$$

Therefore all elements of $F^s(V)$ are roots of $x^{[k]} + \sum_{j=0}^{i} F^s(\alpha_j)x^{[j]}$. Since the degree of this polynomial is $[k]$, the claim follows. ∎

The next lemma shows a connection between the coefficients of the subspace polynomial of a given subspace $V \in \mathcal{G}_q(n,k)$ and the number of its distinct cyclic shifts. To formulate our claim, we need the following equivalence relation.

Definition 4. *For $\alpha, \beta \in \mathbb{F}_{q^n}^*$ and an integer t which divides n, the equivalence relation $\sim_t$ is defined as follows*

$$\alpha \sim_t \beta \iff \frac{\alpha}{\beta} \in \mathbb{F}_{q^t}.$$

Clearly, if $\alpha \sim_t \beta$ then $\alpha \in \beta\mathbb{F}_{q^t}^* \cap \alpha\mathbb{F}_{q^t}^*$, and since all the cyclic shifts of $\mathbb{F}_{q^t}^*$ in $\mathbb{F}_{q^n}^*$ are disjoint, it follows that $\beta\mathbb{F}_{q^t}^* = \alpha\mathbb{F}_{q^t}^*$. Hence, the equivalence classes under this relation are all the cyclic shifts of $\mathbb{F}_{q^t}^*$ in $\mathbb{F}_{q^n}^*$. Therefore, there are exactly $\frac{q^n-1}{q^t-1}$ equivalence classes of $\sim_t$, each of which is of size $q^t - 1$.

Lemma 7. *Let $V \in \mathcal{G}_q(n,k)$ and $P_V(x) = x^{[k]} + \sum_{j=0}^i \alpha_j x^{[j]}$. If $\alpha_s \neq 0$ for some $s \in \{1, \ldots, i\}$ and $\gcd(s,n) = t$ then $\alpha V \neq \beta V$ for all $\alpha, \beta \in \mathbb{F}_{q^n}^*$ such that $\alpha \not\sim_t \beta$.*

Proof: Assume for contradiction that $\alpha V = \beta V$ for some $\alpha, \beta \in \mathbb{F}_{q^n}^*$, where $\alpha \not\sim_t \beta$. By Lemma 5

$$P_{\alpha V}(x) = x^{[k]} + \sum_{j=0}^i \alpha_j \cdot \alpha^{[k]-[j]} x^{[j]}$$

$$P_{\beta V}(x) = x^{[k]} + \sum_{j=0}^i \alpha_j \cdot \beta^{[k]-[j]} x^{[j]}.$$

The equality $\alpha V = \beta V$, together with Lemma 2, imply that

$$\begin{cases} \alpha_s \alpha^{[k]-[s]} &= \alpha_s \beta^{[k]-[s]} \\ \alpha_0 \alpha^{[k]-1} &= \alpha_0 \beta^{[k]-1} \end{cases},$$

and since $\alpha_0 \neq 0$ by Lemma 1, it follows that

$$\begin{cases} \left(\frac{\alpha}{\beta}\right)^{[k]-[s]} &= 1 \\ \left(\frac{\alpha}{\beta}\right)^{[k]-1} &= 1 \end{cases}.$$

By dividing the second equation by the first equation, we get $\left(\frac{\alpha}{\beta}\right)^{[s]-1} = 1$. Hence, $\operatorname{ord}(\frac{\alpha}{\beta})| \gcd(q^n - 1, q^s - 1)$. It is well known that in $\mathbb{Z}_{q^n-1}$, $\gcd(q^n - 1, q^s - 1) = q^{\gcd(n,s)} - 1$ (e.g., [11, p. 147, s. 38]). Therefore, $\operatorname{ord}(\frac{\alpha}{\beta})|q^{\gcd(n,s)} - 1$, which implies that $\frac{\alpha}{\beta} \in \mathbb{F}_{q^t}$ since $t = \gcd(n,s)$, and hence $\alpha \sim_t \beta$, a contradiction. ∎

Corollary 3. *Let $V \in \mathcal{G}_q(n,k)$ and $P_V(x) = x^{[k]} + \sum_{j=0}^i \alpha_j x^{[j]}$. If $\alpha_s \neq 0$ for some $s \in \{1, \ldots, i\}$ with $\gcd(s,n) = t$ then V has at least $\frac{q^n-1}{q^t-1}$ distinct cyclic shifts.*

To construct codes with more than one orbit using the Frobenius automorphism, one would like to find a sufficient condition that a certain Frobenius shift is not a cyclic shift. Such a condition can be derived for the special case, where the subspace polynomial is a certain trinomial. The proof of the following lemma is deferred to Appendix A.

Lemma 8. *If $V \in \mathcal{G}_q(n,k)$ and $P_V(x) = x^{[k]} + \alpha_1 x^{[1]} + \alpha_0 x$, where $\alpha_1 \neq 0$, then there exists $\alpha \in \mathbb{F}_{q^n}^*$, $i \in \{0, \ldots, n-1\}$ such that $F^i(V) = \alpha V$ if and only if*

$$\left(\frac{\alpha_0^{\frac{q^k-q}{q-1}}}{\alpha_1^{\frac{q^k-1}{q-1}}}\right)^{q^i-1} = 1.$$

III. Cyclic Subspace Codes

In this section some constructions of cyclic subspace codes are provided. We distinguish between two cases. In Subsection III-A we discuss codes whose codewords have a full length orbit. In Subsection III-B codes whose codewords do not have a full length orbit are discussed.

Definition 5. *Given a subspace* $V \in \mathcal{G}_q(n, k)$, *the set* $\{\alpha V | \alpha \in \mathbb{F}_{q^n}^*\}$ *is called* the orbit of V. *The subspace* V *has a* full length orbit *if* $|\{\alpha V | \alpha \in \mathbb{F}_{q^n}^*\}| = \frac{q^n-1}{q-1}$. *If* V *does not have a full length orbit then it has a* degenerate orbit.

Note, that a cyclic code with a full length orbit cannot have a minimum distance $2k$. This is a simple observation from the fact that each element $\alpha \in \mathbb{F}_{q^n}^*$ appears in exactly $\frac{q^k-1}{q-1}$ codewords.

We will give several simple related results on subspaces and the size of their orbits. The first claim may be extracted from [10, Corollary 3.13]. For completeness we include a shorter self-contained proof.

Lemma 9. *If* $V \in \mathcal{G}_q(n, k)$ *then* $|\{\alpha V \mid \alpha \in \mathbb{F}_{q^n}^*\}| = \frac{q^n-1}{q^t-1}$ *for some* t *which divides* n.

Proof: Let γ be a primitive element in $\mathbb{F}_{q^n}$ and let $\ell \in \mathbb{N}$ be the smallest integer such that $\gamma^\ell V = V$. Clearly, $\ell | q^n - 1$ and it is readily extracted that each $i \in \mathbb{N}$ and each $0 \le s < \ell$ satisfy $\gamma^s V = \gamma^{i\ell+s} V$. Furthermore, for every $s_1, s_2 \in \{0, \ldots, \ell-1\}$ the sets $A_{s_j} \triangleq \{\gamma^{i\ell+s_j} \mid i \in \mathbb{N}\}$ satisfy $|A_{s_1}| = |A_{s_2}|$. Let $\gamma^{i_1 \cdot \ell}, \gamma^{i_2 \cdot \ell} \in A_0$ for some $i_1, i_2 \in \mathbb{N}$. Since $A_0 = \{\gamma^{i\ell} \mid i \in \mathbb{N}\}$ it follows that

$$\left(\gamma^{i_1 \cdot \ell} + \gamma^{i_2 \cdot \ell}\right) V \subseteq \gamma^{i_1 \cdot \ell} V + \gamma^{i_2 \cdot \ell} V = V + V = V,$$

and hence $\gamma^{i_1 \cdot \ell} + \gamma^{i_2 \cdot \ell} \in A_0$, that is, A_0 is closed under addition. Since A_0 is also closed under multiplication, it follows that A_0 is the multiplicative group of some subfield $\mathbb{F}_{q^t}$ of $\mathbb{F}_{q^n}$. Therefore, $|\{\alpha V \mid \alpha \in \mathbb{F}_{q^n}^*\}| = \ell = \frac{q^n-1}{q^t-1}$. ∎

An immediate consequence of Lemma 9 is that the largest possible size of an orbit is $\frac{q^n-1}{q-1}$, which justifies Definition 5. As will be shown in the sequel (see Section III-B), the parameter t from Lemma 9 must also divide k. A formula for the number of orbits of each possible size is given in [8]. Most of the k-dimensional subspaces of $\mathbb{F}_{q^n}$ have full length orbits. The main goal in constructing cyclic codes is to obtain as many orbits as possible in the code. This task will be left for future work. In this work we consider first the existence of cyclic codes with one full length orbit and cyclic codes with multiple full length orbits. Later, we consider the largest cyclic codes for which all the orbits are degenerate.

A. Codes with Full Length Orbits

Lemma 10. *[17, p. 107, Theorem 10] The polynomial* $Q(x) \triangleq x^{[n]} - x$ *is the product of all monic irreducible polynomials over* $\mathbb{F}_q$ *with degree dividing* n.

Theorem 2. *If* $q^k - 1$ *divides* n *and* $x^{[k]-1} + x^{[1]-1} + 1$ *is irreducible over* $\mathbb{F}_q$ *then the polynomial* $x^{[k]} + x^{[1]} + x$ *is a subspace polynomial with respect to* $\mathbb{F}_{q^n}$.

Proof: Assume that $x^{[k]-1} + x^{[1]-1} + 1$ is irreducible over $\mathbb{F}_q$ and its degree divides n. By Lemma 10 $x^{[k]-1} + x^{[1]-1} + 1 | Q(x)$, and hence $x^{[k]} + x^{[1]} + x | Q(x)$. Therefore, $x^{q^k} + x^q + x$ is a subspace polynomial (see Definition 2), i.e., $P_V(x) = x^{[k]} + x^{[1]} + x$ for some subspace V. ∎

Corollary 4. *If* $q^k - 1$ *divides* n, $x^{[k]-1} + x^{[1]-1} + 1$ *is irreducible over* $\mathbb{F}_q$, *and* $V \in \mathcal{G}_q(n, k)$ *is the subspace whose subspace polynomial is* $x^{[k]} + x^{[1]} + x$, *then* $\mathbb{C} \triangleq \{\alpha V \mid \alpha \in \mathbb{F}_{q^n}^*\}$ *is a cyclic subspace code of size* $\frac{q^n-1}{q-1}$ *and minimum distance at*

least $2k - 2$.

Proof: According to Corollary 3, since the coefficient of x^q in P_V is nonzero, there are $\frac{q^n-1}{q-1}$ distinct cyclic shifts in $\mathbb{C}$. By Lemma 5 and Corollary 2, the minimum distance of $\mathbb{C}$ is at least $2k - 2$. ∎

Although there exists an extensive research on irreducible trinomials over finite fields (e.g., [24]), no explicit construction of irreducible trinomials of the above form is known. However, the following examples were easily found using a computer search.

Example 2. *Since the polynomials* $x^{2^k-1} + x + 1$ *are irreducible over* $\mathbb{F}_2$ *for all* $k \in \{2, 3, 4, 6, 7, 15\}$, *it follows that the polynomial* $x^{2^k} + x^2 + x$ *is a subspace polynomial of a subspace* $V \in \mathcal{G}_2\left((2^k - 1)t, k\right)$ *for all* $t \in \mathbb{N}$. *Therefore, the code* $\mathbb{C} \triangleq \{\alpha V \mid \alpha \in \mathbb{F}^*_{q^{(2^k-1)t}}\}$ *is cyclic code of size* $2^{t \cdot (2^k-1)} - 1$ *and minimum distance* $2k - 2$ *in* $\mathcal{G}_2\left((2^k - 1)t, k\right)$.

By using a similar approach we have that for any k and q, cyclic codes in $\mathcal{G}_q(n, k)$ can be explicitly constructed for infinitely many values of n. The construction will make use of the following lemma.

Lemma 11. *If* $f(x) = \prod_{i=1}^t p_i^{\alpha_i}(x)$ *is a polynomial over* $\mathbb{F}_q$ *and* $p_1(x), \ldots, p_t(x)$ *are its irreducible factors in* $\mathbb{F}_q$ *then* $f(x)$ *splits completely in* $\mathbb{F}_{q^n}$ *for* $n = \operatorname{lcm}\{\deg p_i(x)\}_{i=1}^t$.[‡]

Proof: According to [15, Corollary 2.15, p. 52], the splitting field of an irreducible polynomial of degree m over $\mathbb{F}_q$ is $\mathbb{F}_{q^m}$. Therefore, for each $i = 1, \ldots, t$, the splitting field of p_i is $\mathbb{F}_{q^{n_i}}$, where $n_i \triangleq \deg p_i$. For any i, the only finite fields that contain $\mathbb{F}_{q^{n_i}}$ are of the form $\mathbb{F}_{q^r}$ for r such that $n_i | r$. Hence, the smallest field that contains $\mathbb{F}_{q^{n_i}}$ for all i is $\mathbb{F}_{q^n}$. ∎

Theorem 3. *For any* k *and* q *we may explicitly construct a cyclic subspace code of size* $\frac{q^n-1}{q-1}$ *and minimum distance* $2k - 2$ *in* $\mathcal{G}_q(n, k)$ *for infinitely many values of* n.

Proof: By factoring $T(x) \triangleq x^{[k]} + x^{[1]} + x$ and computing the least common multiplier of the degrees of its factors we find the degree of the splitting field of $T(x)$ (see Lemma 11). The subspace V, whose corresponding subspace polynomial is $T(x)$ may be easily found by finding the kernel of the linear transformation defined by T. If $\mathbb{C} \triangleq \{\alpha V \mid \alpha \in \mathbb{F}^*_{q^n}\}$ then by Corollary 3 there are $\frac{q^n-1}{q-1}$ distinct cyclic shifts in $\mathbb{C}$. By Lemma 5 and Corollary 2, the minimum distance of $\mathbb{C}$ is at least $2k - 2$. Infinitely many values of n will are by considering the cyclic shifts of V in all the field extensions of the splitting field. ∎

Remark 2. *Theorem 3 proves Conjecture 1 for infinitely many values of* n.

Remark 3. *The codes implied by Theorems 2 and Theorem 3 cannot be enlarged using the Frobenius isomorphism due to Lemma 8, since for any* $i \in \{0, \ldots, n-1\}$ *we have that the ith Frobenius shift is also a cyclic shift.*

Let $N = t \cdot n$ and let γ be a primitive element in $\mathbb{F}_{q^N}$. Note, that the set $\{0\} \cup \{\gamma^{i(q^N-1)/(q^n-1)}\}_{i=0}^{q^n-2}$ is the unique subfield $\mathbb{F}_{q^n}$ of $\mathbb{F}_{q^N}$. Let V be a subspace of $\mathbb{F}_{q^n}$. Since $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^N}$ we can view the subspace V as a subspace of $\mathbb{F}_{q^N}$ over $\mathbb{F}_q$.

Now, we present a general method for constructing cyclic codes in $\mathcal{G}_q(N, k)$, where $N = t \cdot n$ for some prime n, which have more than one full length orbit. We do so by using the Frobenius automorphism.

[‡]$\operatorname{lcm}\{s_i\}_{i=1}^t$ stands for the least common multiplier of the integers $s_1, \ldots, s_t$.

Lemma 12. *Let n be a prime, $n|N$, $V \in \mathcal{G}_q(N,k)$ and $P_V(x) = x^{[k]} + \alpha_1 x^{[1]} + \alpha_0 x$, where $\alpha_0, \alpha_1 \in \mathbb{F}_{q^n}^*$. If $\alpha_1^{\frac{q^k-1}{q-1}} \nsim_1 \alpha_0^{\frac{q^k-q}{q-1}}$ (see Definition 4) then the code $\mathbb{C} \subseteq \mathcal{G}_q(N,k)$ defined by*

$$\mathbb{C} \triangleq \bigcup_{i=0}^{n-1} \left\{ \alpha \cdot F^i(V) \mid \alpha \in \mathbb{F}_{q^N}^* \right\} \tag{1}$$

is of size $n \cdot \frac{q^N-1}{q-1}$ and minimum distance $2k - 2$.

Proof: The code $\mathbb{C}$ is obviously cyclic. By Lemmas 4, 5, and 6, the dimension of the intersection between any two distinct subspaces in $\mathbb{C}$ is at most 1, and hence the minimum distance of $\mathbb{C}$ is $2k - 2$.

To show that $|\mathbb{C}| = n \cdot \frac{q^N-1}{q-1}$, fix i and notice that by Lemma 6 we have that the coefficient of $x^{[1]}$ in $P_{F^i(V)}(x)$ is non-zero. Therefore, Lemma 7 implies that the set $\{\alpha \cdot F^i(V) \mid \alpha \in \mathbb{F}_{q^N}^*\}$ consists of $\frac{q^N-1}{q-1}$ distinct subspaces.

To complete the proof, we have to show that all the sets in the union in (1) are disjoint. Let $i, j \in \{0, \dots, n-1\}, i \neq j$, and assume for contradiction that there exists $\beta, \gamma \in \mathbb{F}_{q^N}^*$ such that $\beta F^i(V) = \gamma F^j(V)$. W.l.o.g assume that $j > i$, and denote $U \triangleq F^i(V)$. Notice that by Lemma 6 we have

$$P_U(x) = P_{F^i(V)}(x) = x^{[k]} + F^i(\alpha_1) \cdot x^{[1]} + F^i(\alpha_0) \cdot x = x^{[k]} + \alpha_1^{[i]} \cdot x^{[1]} + \alpha_0^{[i]} \cdot x.$$

Since $F^{j-i}(U) = \frac{\beta}{\gamma} \cdot U$, we may apply Lemma 8 to get

$$\left(\frac{\left(\alpha_0^{q^i}\right)^{\frac{q^k-q}{q-1}}}{\left(\alpha_1^{q^i}\right)^{\frac{q^k-1}{q-1}}} \right)^{q^{j-i}-1} = 1. \tag{2}$$

Denote $z \triangleq \frac{\alpha_0^{\frac{q^k-q}{q-1}}}{\alpha_1^{\frac{q^k-1}{q-1}}}$ and notice that

A1. Equation (2) implies $z^{q^i(q^{j-i}-1)} = 1$.
A2. The condition $\alpha_1^{\frac{q^k-1}{q-1}} \nsim_1 \alpha_0^{\frac{q^k-q}{q-1}}$ implies $z \notin \mathbb{F}_q$.
A3. Since $\alpha_0, \alpha_1 \in \mathbb{F}_{q^n}^*$ it follows that $z \in \mathbb{F}_{q^n}^*$.

By A1 and A3 we have that $\mathrm{ord}(z)$ divides both $q^i(q^{j-i}-1)$ and $q^n - 1$, therefore $\mathrm{ord}(z)|gcd(q^i(q^{j-i}-1), q^n-1)$. Since $q^n - 1$ is not a power of q, it follows that $gcd(q^n-1, q^i) = 1$, and hence,

$$gcd(q^i(q^{j-i}-1), q^n-1) = gcd(q^{j-i}-1, q^n-1).$$

It is well known that in any field $gcd(x^r - 1, x^s - 1) = x^{gcd(r,s)} - 1$ (e.g., [11, p. 147, s. 38]). Therefore, the primality of n implies that $gcd(q^{j-i} - 1, q^n - 1) = q^{gcd(j-i,n)} - 1 = q - 1$, and hence $\mathrm{ord}(z)|q - 1$. The only elements of $\mathbb{F}_{q^N}$ whose order divides $q - 1$ are the elements of $\mathbb{F}_q$, and hence $z \in \mathbb{F}_q$, a contradiction to A2. ∎

Lemma 13 which follows, whose proof is deferred to Appendix A, shows that coefficients α_0, α_1 from Lemma 12 may be easily found in $\mathbb{F}_{q^n}$.

Lemma 13. *Let n be prime and let γ be a primitive element in $\mathbb{F}_{q^n}$. If $\alpha_0 \triangleq \gamma$ and $\alpha_1 \triangleq \gamma^q$ then $\alpha_1^{\frac{q^k-1}{q-1}} \nsim_1 \alpha_0^{\frac{q^k-q}{q-1}}$.*

As a consequence of Lemma 12 and Lemma 13 we have the following theorem.

Theorem 4. *Let n be prime, γ a primitive element of $\mathbb{F}_{q^n}$, and define $\alpha_0 \triangleq \gamma$ and $\alpha_1 \triangleq \gamma^q$. If $\mathbb{F}_{q^N}$ is the splitting field of the polynomial $x^{[k]} + \alpha_1 x^{[1]} + \alpha_0 x$ and $V \in \mathcal{G}_q(N, k)$ its corresponding subspace, then*

$$\mathbb{C} \triangleq \bigcup_{i=0}^{n-1} \left\{ \alpha \cdot F^i(V) \mid \alpha \in \mathbb{F}_{q^N}^* \right\}$$

is a cyclic code of size $n \cdot \frac{q^N - 1}{q - 1}$ and minimum distance $2k - 2$.

Note that the construction in Theorem 4 improves the construction of Theorem 3. In Theorem 3 we construct a code with one full length orbit, where in Theorem 4 we add multiple orbits without compromising the minimum distance.

B. Codes with degenerate orbits

In this subsection it is shown that subspaces of $\mathcal{G}_q(n, k)$ that may be considered as subspaces over a subfield of $\mathbb{F}_{q^n}$ which is larger than $\mathbb{F}_q$, form a cyclic code with a unique subspace polynomial structure. The cyclic property and the minimum distance of this code are an immediate consequence of this unique structure.

Lemma 14. *If $n, k \in \mathbb{N}, k < n$ and $d \in \mathbb{N}$ divides $\gcd(n, k)$, then there exists an $\mathbb{F}_{q^d}$-homomorphism from $\mathcal{G}_{q^d}(n/d, k/d)$ to $\mathcal{G}_q(n, k)$.*

Proof: Let $\mathbb{F}_{q^d}^{n/d}$ be the vector space of dimension n/d over q^d. It is widely known that there exists an isomorphism f from $\mathbb{F}_{q^d}^{n/d}$ to $\mathbb{F}_{(q^d)^{n/d}}$. Notice that by our abuse of notation, both $\mathbb{F}_{q^d}^{n/d}$ and $\mathbb{F}_{(q^d)^{n/d}}$ can be considered as vector spaces over $\mathbb{F}_{q^d}$. Since there is a unique field with q^n elements, $\mathbb{F}_{q^n}$ may also be considered as a vector space over $\mathbb{F}_{q^d}$. Therefore, there exists an isomorphism $g : \mathbb{F}_{q^d}^{n/d} \to \mathbb{F}_{q^n}$ such that $g \triangleq h \circ f$, where h is some isomorphism from $\mathbb{F}_{(q^d)^{n/d}}$ to $\mathbb{F}_{q^n}$.

Notice that for all $u, v \in \mathbb{F}_{q^d}^{n/d}$ and $\alpha, \beta \in \mathbb{F}_{q^d}$, we have $g(\alpha v + \beta u) = \alpha g(v) + \beta g(u)$. For $V \in \mathcal{G}_{q^d}(n/d, k/d)$ let $G(V) \triangleq \{g(v) | v \in V\}$. The set $G(V)$ is clearly a subspace of dimension k over $\mathbb{F}_q$ in $\mathbb{F}_{q^n}$. Furthermore, the function $G : \mathcal{G}_{q^d}(n/d, k/d) \to \mathcal{G}_q(n, k)$ is injective since g is injective. ∎

Lemma 14 allows us to define the following set of subspaces.

Construction 1. *For $n, k \in \mathbb{N}$ and $d \in \mathbb{N}$ such that $d | \gcd(n, k)$, let $\mathbb{C}_d$ be the code*

$$\{G(V) | V \in \mathcal{G}_{q^d}(n/d, k/d)\},$$

where G was defined in the proof of Lemma 14.

Since $\mathbb{C}_d$ is the image of an injective function from $\mathcal{G}_{q^d}(n/d, k/d)$ to $\mathcal{G}_q(n, k)$, we have the following.

Corollary 5. $|\mathbb{C}_d| = \begin{bmatrix} n/d \\ k/d \end{bmatrix}_{q^d}$.

Remark 4. *The code $\mathbb{C}_d$ from construction 1 may be alternatively defined as*

$$\mathbb{C}_d \triangleq \left\{ \sum_{i=1}^{k/d} \alpha_i \mathbb{F}_{q^d} \;\middle|\; \alpha_1, \dots, \alpha_{k/d} \in \mathbb{F}_{q^n} \text{ are linearly independent over } \mathbb{F}_{q^d} \right\}.$$

The proof of the equivalence of this alternative definition appears in Appendix B. The code $\mathbb{C}_d$ may also be defined as the set of all subspaces of $\mathcal{G}_q(n, k)$ that are also subspaces over $\mathbb{F}_{q^d}$.

The subspaces in $\mathbb{C}_d$ admit a unique subspace polynomial structure, from which the useful properties of $\mathbb{C}_d$ are apparent.

Lemma 15. *If $V \in \mathcal{G}_q(n,k)$ then $V \in \mathbb{C}_d$ if and only if $P_V(x) = \sum_{i=0}^{k/d} c_i x^{[di]}$ for some c_i's in $\mathbb{F}_{q^n}$.*

Proof: Let $V \in \mathbb{C}_d$, and let $U \in \mathcal{G}_{q^d}(n/d, k/d)$ be such that $F(U) = V$ (see Construction 1). By Definition 2 it follows that $P_U | x^{(q^d)^{n/d}} - x$. Since $x^{(q^d)^{n/d}} - x = x^{[n]} - x$, it follows that P_U is a subspace polynomial of a subspace $W \in \mathcal{G}_q(n,k)$. The roots of P_U are precisely the set $\{g(u) | u \in U\}$, where g is the isomorphism between $\mathbb{F}_{q^d}^{n/d}$ and $\mathbb{F}_{q^n}$ mentioned in the proof of Lemma 14, and hence, $W = V$. Since P_U is a subspace polynomial of a subspace in $\mathcal{G}_{q^d}(n/d, k/d)$, its subspace polynomial is of the form $P_U(x) = \sum_{i=0}^{k/d} c_i x^{(q^d)^i}$. Since $P_V = P_U$, the claim follows.

Conversely, let $V \in \mathcal{G}_q(n,k)$ with $P_V(x) = \sum_{i=0}^{k/d} c_i x^{[di]}$. By Definition 2, it follows that $P_V | x^{[n]} - x$, and thus $P_V | x^{(q^d)^{n/d}} - x$. Therefore P_V is a subspace polynomial of some $U \in \mathcal{G}_{q^d}(n/d, k/d)$, and hence $V \in \mathbb{C}_d$. ∎

Corollary 6. $\mathbb{C}_d \subseteq \mathcal{G}_q(n,k)$ *is a cyclic subspace code.*

Proof: Let $V \in \mathbb{C}_d$ and $\alpha \in \mathbb{F}_{q^n}^*$. By Lemma 15 the subspace polynomial of V is of the form $P_V(x) = \sum_{i=0}^{k/d} c_i x^{[di]}$ for some $c_i \in \mathbb{F}_{q^n}$. By Lemma 5 the subspace polynomial of αV is $P_V(x) = \sum_{i=0}^{k/d} c_i \alpha^{[k]-[di]} x^{[di]}$. Again by Lemma 15, it follows that $\alpha V \in \mathbb{C}_d$. ∎

Since for $V \in \mathbb{C}_d$ we have that $\mathrm{gap}(V) \geq d$, and the following result is a consequence of Corollary 2 and Definition 3.

Corollary 7. *The minimum distance of $\mathbb{C}_d$ is $2d$.*

The structure of the subspace polynomials of the codewords of $\mathbb{C}_d$ allows us to construct a code $\mathbb{C}$ which is a union of $\mathbb{C}_{d_i}$ for distinct d_i's which divide $\gcd(n,k)$. We now analyze the size and distance of the resulting code.

Lemma 16. *Let $k,n \in \mathbb{N}, k < n$. If $d_1, \ldots, d_t$ divide both n and k and $d = \mathrm{lcm}(d_1, \ldots, d_t)$ then $\bigcap_{i=1}^{t} \mathbb{C}_{d_i} = \mathbb{C}_d$.*

Proof: According to Lemma 15 if $V \in \mathbb{C}_d$ then $P_V(x) = \sum_{i=0}^{k/d} c_i x^{[id]}$. Since $d_j | d$ for each j, we may also write $P_V(x) = \sum_{i=0}^{k/d_j} c_i' x^{[id_j]}$, where all additional coefficients are 0, and thus $V \in \mathbb{C}_{d_j}$ for each j.

On the other hand, if $V \in \bigcap_{i=1}^{t} \mathbb{C}_{d_i}$, again by Lemma 15 it follows that all nonzero coefficients of P_V correspond to $x^{[\ell]}$ such that $d_j | \ell$ for each j. Thus, $d | \ell$ and $V \in \mathbb{C}_d$. ∎

Construction 2. *Let $k,n \in \mathbb{N}, k < n$. If $d_1, \ldots, d_t$ divide both n and k then let $\mathbb{C} \triangleq \bigcup_{i=1}^{t} \mathbb{C}_{d_i}$.*

Lemma 17. *$\mathbb{C}$ is a cyclic code of with codewords of dimension k and minimum distance $2\min\{d_i\}_{i=1}^{t}$. The size of $\mathbb{C}$ is given by*

$$|\mathbb{C}| = \sum_{i=1}^{t} \begin{bmatrix} n/d_i \\ k/d_i \end{bmatrix}_{q^{d_i}} - \sum_{i<j} \begin{bmatrix} n/\mathrm{lcm}(d_i, d_j) \\ k/\mathrm{lcm}(d_i, d_j) \end{bmatrix}_{q^{\mathrm{lcm}(d_i,d_j)}} + \sum_{i<j<\ell} \begin{bmatrix} n/\mathrm{lcm}(d_i, d_j, d_\ell) \\ k/\mathrm{lcm}(d_i, d_j, d_\ell) \end{bmatrix}_{q^{\mathrm{lcm}(d_i,d_j,d_\ell)}} - \cdots.$$

Proof: By Corollary 7 we have that $gap(V) \geq \min\{d_i\}_{i=1}^{t}$ for each $V \in \mathbb{C}$, and hence the minimum distance of $\mathbb{C}$ is at least $2\min\{d_i\}_{i=1}^{t}$ by Corollary 2. By Corollary 5 we have that $|\mathbb{C}_{d_i}| = \begin{bmatrix} n/d_i \\ k/d_i \end{bmatrix}_{q^{d_i}}$ for each i. Furthermore, by Lemma 16 the size of the intersection of $\mathbb{C}_{d_{i_1}}, \ldots, \mathbb{C}_{d_{i_\ell}}$ is $\begin{bmatrix} n/d \\ k/d \end{bmatrix}_{q^d}$ where $d = \mathrm{lcm}(d_{i_1}, \ldots, d_{i_\ell})$. These facts allow us to obtain the exact size of $\mathbb{C}$ using the inclusion-exclusion principle [16, Chapter 10]. ∎

Using similar techniques, we show that a cyclic code over a large field may be embedded in a Grassmannian over a smaller field, while preserving cyclicity and multiplying the minimal distance by some factor. Note that Construction 1 is a special case of this technique, where the embedded code is $\mathcal{G}_{q^d}(n/d, k/d)$.

Theorem 5. *Let d be an integer such that $d | \gcd(n,k)$. If $\mathbb{C} \subseteq \mathcal{G}_{q^d}(n/d, k/d)$ is a cyclic code with minimum distance*

$2 \cdot (k/d) - 2\delta$ *then there exists a cyclic code* $\mathbb{C}' \subseteq \mathcal{G}_q(n, k)$ *of size* $|\mathbb{C}|$ *and minimum distance* $2k - 2d\delta$.

Proof: Let $g : \mathbb{F}_{q^d}^{n/d} \to \mathbb{F}_{q^n}$ and $G : \mathcal{G}_{q^d}(n/d, k/d) \to \mathcal{G}_q(n, k)$ be the embeddings defined in the proof of Lemma 14. If $\mathbb{C}' \triangleq \{G(V)|V \in \mathbb{C}\}$ then $|\mathbb{C}'| = |\mathbb{C}|$, since G is injective. The cyclic property of $\mathbb{C}'$ follows from the fact that $P_V(x) = P_{G(V)}(x)$ for all $V \in \mathbb{C}$, as shown in the proof of Lemma 15. To bound the minimum distance of $\mathbb{C}'$ it suffices to show that if $U_1, U_2 \in \mathbb{C}$ then

$$\dim(G(U_1) \cap G(U_2)) = d \cdot \dim(U_1, U_2).$$

Indeed, if $w \triangleq \dim(U_1 \cap U_2)$, then since g is an isomorphism of subspaces over $\mathbb{F}_{q^d}$, it follows that the set $Z \triangleq \{g(z)|z \in U_1 \cap U_2\}$ is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. By a simple counting argument, $\dim Z = dw$, and hence, $\dim(F(U_1) \cap F(U_2)) \geq dw$. Assuming for contradiction that $\dim(F(U_1) \cap F(U_2)) > dw$ clearly implies that $\dim(U_1 \cap U_2) > w$, a contradiction. ∎

IV. Conclusions and Future Work

In this paper we have considered constructions of cyclic subspace codes. We have proved the existence of a cyclic code in $\mathcal{G}_q(n, k)$ for any given k and infinitely many values of n. The constructed codes have minimum subspace distance $2k - 2$, the normalizer of a Singer subgroup is their automorphism group if n is a prime, and they have full length orbits for all values of n. We have also constructed large codes when all the orbits are degenerated. We have shown how the representation of subspaces by their subspace polynomials can be used in constructing subspace codes.

For future research, the main problems are to construct cyclic codes of large size, to explore the structure and properties of our codes, and to examine possible decoding algorithms for them. It is easily verified that the vast majority of subspaces have full length orbits. Therefore, it seems reasonable to conjecture that full length orbits with minimum distance $2k - 2$ exist for any value of n, k, q (see Conjecture 1). Although the codes presented in Section III-A are the first known explicit construction of such codes, they are most likely the tip of the iceberg, and codes of these parameters are abound.

Although the gap of two polynomials provides significant information about the intersection of their respective subspaces, Remark 1 shows that the gap might not be the most efficient tool for this purpose. Therefore, another open problem is finding a better measure for the intersection of two subspaces, and in particular, two subspaces from the same orbit.

A prominent part of the study of subspace polynomials relies on understanding the connection between the coefficients of a polynomial and the size of the respective splitting field. Hence, any progress in this direction may provide an improvement of our results.

References

[1] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, "On perfect codes and related concepts," *Designs, Codes and Cryptography*, vol 22, pp. 221–237, 2001.

[2] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, "Subspace polynomials and cyclic subspace codes," *arXiv:1404.7739*, 2014.

[3] E. Ben-Sasson, and S. Kopparty, "Affine dispersers from subspace polynomials," *SIAM Journal on Computing*, vol. 41, pp. 880–914, 2012.

[4] E. Ben-Sasson, S. Kopparty, and J. Radhakrishnan, "Subspace polynomials and limits to list decoding of Reed-Solomon codes," *IEEE Transactions on Information Theory,*, vol. 56, pp. 113–120, 2010.

[5] M. Braun, T. Etzion, P. Ostergard, A. Vardy, and A. Wasserman, "Existence of q-analogs of Steiner systems," *arXiv:1304.1462*, 2013.

[6] Q. Cheng, S. Gao, and D. Wan, "Constructing high order elements through subspace polynomials," *Proceedings of the Twenty-third Annual ACM-SIAM Symposium on Discrete Algorithms (SODA),* pp. 1547–1463, 2012.

[7] L. Chihara, "On the zeros of the Askey-Wilson polynomials, with applications to coding theory," *SIAM Journal on Mathematical Analysis,* vol. 18, pp. 191-207, 1987.

[8] K. Drudge, "On the orbits of Singer groups and their subgroups," *Electronic Journal of Combinatorics*, vol. 9, 2002.

[9] T. Etzion, and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, pp. 1165-1173, 2011.

[10] H. Gluesing-Luerssen, and K. Morrison, and C. Troha, "Cyclic orbit codes and stabilizer subfields," *arXiv:1403.1218*, 2013.

[11] R. L. Graham, D. E. Knuth, and O. Patashnik, "Concrete Mathematics: A Foundation for Computer Science," *Addison-Wesley*, 1994

[12] B. Huppert, "Endliche Gruppen," *I, Springer-Verlag*, Berlin, 1967.

[13] R. Koetter and F. R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Transactions on Information Theory*, vol. 54, pp. 3579–3591, 2008.

[14] A. Kohnert, and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," *Lecture Notes Computer Science*, vol. 5395, pp. 31–42, 2008.

[15] R. Lidl, and H. Niederreiter, "Finite Fields" *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, vol. 20, 1997.

[16] J. H. van Lint and R. M. Wilson, "A course in combinatorics" *Cambridge university press*, 2001.

[17] F.J. MacWilliams, and N.J. Sloane, "The Theory of Error-correcting Codes: Part 2," *Elsevier*, vol. 16, 1977.

[18] W. J. Martin, and X. J. Zhu, "Anticodes for the Grassman and bilinear forms graphs," *Designs, Codes and Cryptography,* vol. 6, pp. 73-79, 1995.

[19] O. Ore, "On a special class of polynomials," *Transactions of the American Mathematical Society*, vol. 35, pp. 559–584, 1933.

[20] D. Silva, F.R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory,*, vol. 54, pp. 3951–3967, 2008.

[21] M. Schwartz, and T. Etzion, "Codes and anticodes in the Grassman graph," *Journal of Combinatorial Theory,* Series A, vol 97, pp. 27–42, 2002.

[22] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, "Cyclic orbit codes," *IEEE Transactions on Information Theory*, vol. 59, pp. 7386–7404, 2013.

[23] A. Wachter-Zeh, "Bounds on list decoding of rank-metric codes," *IEEE Transactions on Information Theory*, vol. 59, pp. 7268–7277, 2013.

[24] J. von zur Gathen, "Irreducible trinomials over finite fields," *Mathematics of Computation*, vol. 72, pp. 1987–2000, 2003.

APPENDIX A

Proof: (of Lemma 8) Assume $F^i(V) = \alpha V$ for some α. By Lemmas 5 and 6,

$$
\begin{aligned}
P_{\alpha V}(x) &= x^{[k]} + \alpha^{[k]-[1]} \cdot \alpha_1 x^{[1]} + \alpha^{[k]-1} \cdot \alpha_0 x \\
P_{F^i(V)}(x) &= x^{[k]} + F^i(\alpha_1) x^{[1]} + F^i(\alpha_0) x.
\end{aligned}
$$

By Lemma 2,

$$
\begin{cases}
\alpha^{[k]-[1]} \cdot \alpha_1 = F^i(\alpha_1) \\
\alpha^{[k]-1} \cdot \alpha_0 = F^i(\alpha_0)
\end{cases}
$$

$$
\begin{cases}
\alpha^{[k]-[1]} \cdot \alpha_1 = \alpha_1^{[i]} \\
\alpha^{[k]-1} \cdot \alpha_0 = \alpha_0^{[i]}
\end{cases}
$$

Since $\alpha_0 \neq 0$ (by Lemma 1) and $\alpha_1 \neq 0$, $\alpha^{[1]-1} = \left(\frac{\alpha_0}{\alpha_1}\right)^{q^i-1}$. Using some algebraic manipulations we have,

$$\alpha^{[k]-[1]} = \alpha_1^{[i]-1}$$

$$\alpha^{(q-1)\left(\frac{q^k-q}{q-1}\right)} = \alpha_1^{q^i-1}$$

$$\left(\frac{\alpha_0}{\alpha_1}\right)^{(q^i-1)\left(\frac{q^k-q}{q-1}\right)} = \alpha_1^{q^i-1}$$

$$\frac{\alpha_0^{\frac{q^k-q}{q-1}\cdot(q^i-1)}}{\alpha_1^{\frac{q^k-q}{q-1}\cdot(q^i-1)+(q^i-1)}} = 1$$

$$\frac{\alpha_0^{\frac{q^k-q}{q-1}\cdot(q^i-1)}}{\alpha_1^{\frac{q^k-1}{q-1}\cdot(q^i-1)}} = 1$$

$$\left(\frac{\alpha_0^{\frac{q^k-q}{q-1}}}{\alpha_1^{\frac{q^k-1}{q-1}}}\right)^{q^i-1} = 1,$$

which concludes the proof of one direction of the lemma. Now assume

$$\left(\frac{\alpha_0^{\frac{q^k-q}{q-1}}}{\alpha_1^{\frac{q^k-1}{q-1}}}\right)^{q^i-1} = 1.$$

Define $\alpha \triangleq \left(\frac{\alpha_0}{\alpha_1}\right)^{\frac{q^i-1}{q-1}}$. We get

$$\left(\frac{\alpha_0^{\frac{q^k-q}{q-1}}}{\alpha_1^{\frac{q^k-1}{q-1}}}\right)^{q^i-1} = 1$$

$$\left(\frac{\alpha_0^{\frac{q^k-q}{q-1}}}{\alpha_1^{\frac{q^k-q}{q-1}}\cdot\alpha_1}\right)^{q^i-1} = 1$$

$$\left(\frac{\alpha_0^{\frac{q^i-1}{q-1}}}{\alpha_1^{\frac{q^i-1}{q-1}}}\right)^{q^k-q} = \alpha_1^{q^i-1}$$

$$\alpha^{q^k-q} = \alpha_1^{q^i-1}.$$

In addition, we have $\alpha^{q^k-1} = \alpha^{q^k-q}\alpha^{q-1} = \left(\alpha_1^{q^i-1}\right)\cdot\left(\frac{\alpha_0^{q^i-1}}{\alpha_1^{q^i-1}}\right) = \alpha_0^{q^i-1}$. Therefore:

$$\begin{cases} \alpha^{q^k-q} = \alpha_1^{q^i-1} \\ \alpha^{q^k-1} = \alpha_0^{q^i-1} \end{cases}$$

$$\begin{cases} \alpha^{q^k-q}\cdot\alpha_1 = \alpha_1^{q^i} \\ \alpha^{q^k-1}\cdot\alpha_0 = \alpha_0^{q^i} \end{cases},$$

which implies that $F^i(V) = \alpha V$ due to equality between the coefficients of the corresponding subspace polynomials. ∎

Proof: (of Lemma 13) Assume for contradiction that

$$\alpha_0^{\frac{q^k-q}{q-1}} \sim_1 \alpha_1^{\frac{q^k-1}{q-1}},$$

i.e., there exists $\alpha \in \mathbb{F}_q^*$ such that

$$\alpha \cdot \gamma^{\frac{q^k-q}{q-1}} = (\gamma^q)^{\frac{q^k-1}{q-1}} . \tag{3}$$

Raising both sides of (3) by the $(q-1)$th power yields

$$\gamma^{q^k-q} = \gamma^{q^{k+1}-q}$$
$$\gamma^{q^k(q-1)} = 1. \tag{4}$$

Since $q \in \mathbb{Z}_{q^n-1}^*$, it follows that q has a multiplicative inverse w modulo $q^n - 1$. By raising both sides of (4) by the w^kth power we get that $\gamma^{q-1} = 1$, and hence, $\gamma \in \mathbb{F}_q$, a contradiction. ∎

APPENDIX B

In this appendix we prove the equivalence of an alternative definition to Construction 1 (see Remark 4). The following lemma is required for the proof of equivalence.

Lemma 18. *If $V \in \mathcal{G}_q(n,k)$ may be written as $V = \bigcup_{i=1}^{\ell} \alpha_i \mathbb{F}_{q^d}$, where $d | \gcd(n,k)$, then V may be written as a direct sum $V = \sum_{j=1}^{k/d} \beta_j \mathbb{F}_{q^d}$.*

Proof: We show that for every $J \subseteq \{1, \ldots, \ell\}$, every $\alpha_i \mathbb{F}_{q^d}$ is either contained or mutually disjoint with $A_J \triangleq \sum_{j \in J} \alpha_j \mathbb{F}_{q^d}$. Assume for contradiction that there exists $\alpha_i \mathbb{F}_{q^d}, i \notin J$ that is neither contained nor mutually disjoint with A_J. That is, there exists $u_1, u_2 \in \mathbb{F}_{q^d}^*$ such that $\alpha_i u_1 \in A_J$ and $\alpha_i u_2 \notin A_J$. Since $\alpha_i u_1 \in A_J$ it follows that there exists $s_j \in \mathbb{F}_{q^d}$ for each $j \in J$ such that $\alpha_i u_1 = \sum_{j \in J} \alpha_j s_j$. Hence, $\alpha_i = u_1^{-1} \sum_{j \in J} \alpha_j s_j$ and therefore $\alpha_i u_2 = u_1^{-1} \sum_{j \in J} \alpha_j s_j \cdot u_2$. However, since $u_2/u_1 \in \mathbb{F}_{q^d}^*$ and $s_j \in \mathbb{F}_{q^d}$ for all j, it follows that $\alpha_i u_2 = \sum_{j \in J} \alpha_j (s_j u_2/u_1) \in A_J$, a contradiction. Therefore, by taking $\alpha_1 \mathbb{F}_{q^d}$ and iteratively expanding it by adding disjoint cyclic shifts of $\mathbb{F}_{q^d}$, the required direct sum may be achieved. ∎

Theorem 6. *Let $d \in \mathbb{N}$ such that $d | \gcd(n,k)$. For a subspace $V \in \mathcal{G}_q(n,k)$, $V \in \mathbb{C}_d$ (see Construction 1) if and only if V may be written as a direct sum of cyclic shifts of $\mathbb{F}_{q^d}$.*

Proof: If $V \in \mathbb{C}_d$ then by Lemma 15, $P_V(x) = \sum_{i=0}^{k/d} c_i x^{[id]}$. Since for all $\gamma \in \mathbb{F}_{q^d}$ we have $\gamma^{[d]-1} = 1$, it follows that if $P_V(v) = 0$ for $v \in \mathbb{F}_{q^n}$, then $P_V(\gamma v) = \sum_{i=0}^{k/d} c_i (\gamma v)^{[id]} = P_V(v) = 0$. Therefore, V is a union of cyclic shifts of $\mathbb{F}_{q^d}$, and according to Lemma 18 may be written as a direct sum of cyclic shifts of $\mathbb{F}_{q^d}$.

On the other hand, if $V = \sum_{i=1}^{k/d} \alpha_i \mathbb{F}_{q^d}$ such that $\alpha_i \in \mathbb{F}_{q^n}$, let $\beta_i \in \mathbb{F}_{q^d}^{n/d}, i \in \{1, \ldots, k/d\}$ such that $\beta_i \triangleq g^{-1}(\alpha_i)$, where g is the isomorphism between $\mathbb{F}_{q^d}^{n/d}$ and $\mathbb{F}_{q^n}$ mentioned in the proof of Lemma 14. Let U be the linear span of $\{\beta_i\}_{i=1}^{k/d}$ in $\mathbb{F}_{q^d}^{n/d}$ over $\mathbb{F}_{q^d}$. We show that U is a $\frac{k}{d}$-subspace. Assume for contradiction that the elements of $\{\beta_i\}_{i=1}^{k/d}$ are linearly dependent, i.e., there exists $\gamma_i \in \mathbb{F}_{q^d}$ such that $\sum \gamma_i \beta_i = 0$. Hence, $0 = g(0) = g(\sum \gamma_i \beta_i) = \sum \gamma_i \alpha_i$ and therefore, the element $0 \in \mathbb{F}_{q^n}$ has two distinct representations as an element of V. This implies that $|V| < q^k$, a contradiction. Now observe that,

$$\begin{aligned} G(U) &= \{g(u) \mid u \in U\} \\ &= \left\{ g\left(\sum \gamma_i \beta_i \right) \mid \forall i, \gamma_i \in \mathbb{F}_{q^d} \right\} \\ &= \left\{ \sum \gamma_i \alpha_i \mid \forall i, \gamma_i \in \mathbb{F}_{q^d} \right\} = \sum \alpha_i \mathbb{F}_{q^d} = V, \end{aligned}$$

and hence $V \in \mathbb{C}_d$. ∎