On Linear Subspace Codes Closed under Intersection

Pranab Basu[†] Navin Kashyap[†]

***Abstract*—Subspace codes are subsets of the projective space $\mathbb{P}_q(n)$, which is the set of all subspaces of the vector space $\mathbb{F}_q^n$. Koetter and Kschischang argued that subspace codes are useful for error and erasure correction in random network coding. Linearity in subspace codes was defined by Braun, Etzion and Vardy, and they conjectured that the largest cardinality of a linear subspace code in $\mathbb{P}_q(n)$ is 2^n. In this paper, we show that the conjecture holds for linear subspace codes that are closed under intersection, i.e., codes having the property that the intersection of any pair of codewords is also a codeword. The proof is via a characterization of such codes in terms of partitions of linearly independent subsets of $\mathbb{F}_q^n$.**

I. Introduction

Let $\mathbb{F}_q^n$ be the vector space of dimension n over the field $\mathbb{F}_q$ of order q. The set of all subspaces of $\mathbb{F}_q^n$ is called the *projective space* of order n over $\mathbb{F}_q$ and is denoted by $\mathbb{P}_q(n)$. The subspace distance function in a projective space is defined as follows: for $X, Y \in \mathbb{P}_q(n)$,

$$d_S(X,Y) := \dim X + \dim Y - 2\dim(X \cap Y).$$

The subspace distance measure d_S turns $\mathbb{P}_q(n)$ into a metric space [1]. An (n, M, d) code in the projective space $\mathbb{P}_q(n)$ is defined to be any $\mathbb{C} \subseteq \mathbb{P}_q(n)$ such that $|\mathbb{C}| = M$ and $d_S(X,Y) \geq d$ for all $X, Y \in \mathbb{C}$. Any such code $\mathbb{C}$ is also called a *subspace code*.

Koetter and Kschischang showed [1] that subspace codes defined in projective space $\mathbb{P}_q(n)$ are useful for error and erasure correction in random networks. To be precise, they showed that an (n, M, d) code is capable of correcting any combination of t packet errors as well as ρ packet erasures introduced anywhere within the network, as long as $2(t+\rho) < d$. Thus, a natural analogy can be drawn between error and erasure correction in random network coding and that in classical coding over $\mathbb{F}_q^n$. It makes sense to use this analogy to develop aspects of subspace codes along the same lines as those of classical error-correcting codes. Indeed, there has been much prior work in this spirit, for example, bounds of the Gilbert-Varshamov type [3] and the Singleton type [11] have been derived for subspace codes. Other aspects of these codes have been explored in the existing literature — see e.g., [1], [4], [5], [6], [7], [8], [9], [10].

A notion that has proved to be enormously useful in classical coding is that of linearity. Recall that a linear code is simply a linear subspace of $\mathbb{F}_q^n$. In particular, a linear code forms an abelian group under the usual componentwise addition over $\mathbb{F}_q$. Linear codes have a concise representation in terms of generator and parity-check matrices, which, among other things, lead to relatively simple encoding and decoding algorithms — see e.g., [13]. Extending, by analogy, the notion of linearity to subspace codes should prove similarly useful. However, this has proved to be difficult. This is mainly due to one crucial difference between the projective space $\mathbb{P}_q(n)$ equipped with the subspace distance measure and the *Hamming space* of $\mathbb{F}_q^n$ equipped with the Hamming distance measure. While Hamming distance is translation-invariant, there is no equivalent notion applicable to projective space as a whole, under subspace distance.

Nonetheless, as described in [2], it is possible to define a certain type of linearity in projective space as well. The authors of [2] defined a linear subspace code in $\mathbb{P}_q(n)$ to be a subset $\mathcal{C} \subseteq \mathbb{P}_q(n)$ which can be endowed with a binary operation $\boxplus$ that makes $\mathcal{C}$ an abelian group having the property that the subspace distance measure restricted to $\mathcal{C}$ is translation-invariant. They gave various constructions of linear codes in $\mathbb{P}_q(n)$ including one that is generated by basis vectors of the ambient space $\mathbb{F}_q^n$. A code constructed in this manner was termed *a code derived from a fixed basis* in [12]. It was conjectured in [2] that a linear subspace code in $\mathbb{P}_q(n)$ can have at most 2^n codewords. Another conjecture was made about the linear codes in $\mathbb{P}_q(n)$ that contain $\mathbb{F}_q^n$ as a codeword, which states that any such linear code can have at most $\binom{n}{k}$ k-dimensional codewords, for $0 \leq k \leq n$. The last conjecture was very recently proved in [12] using a result of Lovasz [14]. It was also shown that the codes attaining the bound stated in this conjecture must be derived from a fixed basis. However, it should be noted that there are examples of linear codes that do not contain $\mathbb{F}_q^n$ as a codeword, and yet attain the conjectured maximum possible cardinality of 2^n [2].

In this paper, we focus on the class of linear subspace codes which are closed under the usual set/subspace intersection operation, i.e., linear subspace codes with the property that the intersection of any pair of codewords is also a codeword. We describe a method of constructing such codes from partitions of linearly independent subsets of $\mathbb{F}_q^n$. We say that a code constructed in this manner is *derived from a partition of a linearly independent set*. Codes derived from a fixed basis form special cases of our construction. We go on to show that

[†]P. Basu and N. Kashyap are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore. Email: colonel.pranab@gmail.com, nkashyap@ece.iisc.ernet.in.

978-1-4799-6619-6/15/$31.00 © 2015 IEEE

any linear subspace code that is closed under intersection must be derived from a partition of a linearly independent set. This yields a complete characterization of this class of subspace codes. From this characterization, it is straightforward to deduce that the conjecture of Braun, Etzion and Vardy [2] on the maximum cardinality of a linear subspace code holds for the class of linear codes closed under intersection.

The rest of the paper is organized as follows. Section II introduces the reader to the formal definitions related to linear subspace codes and the conjectures made in [2]. The class of linear codes in $\mathbb{P}_q(n)$ closed under intersection are defined in Section III and their characterization as codes derived from a partition of a linearly independent set is proved. In Section IV, we study the maximal members of the class of codes of interest to us. It is shown here that the maximal such codes are precisely those that are derived from a fixed basis. Along the way, we show that the maximum cardinality of any linear code closed under intersection is 2^n, thus verifying the Braun-Etzion-Vardy conjecture for this class of subspace codes. Section V contains a few concluding remarks.

II. Linear Codes in Projective Space

Braun, Etzion and Vardy [2] introduced a notion of linearity in projective space by abstracting the key properties of linear codes in the Hamming space $\mathbb{F}_2^n$. A linear code in $\mathbb{P}_q(n)$ is defined as follows:

Definition 1. *A subset $\mathcal{U} \subseteq \mathbb{P}_q(n)$, with $\{\mathbf{0}\} \in \mathcal{U}$, is a* linear subspace code *if the following properties hold:*
(i) there exists a function $\boxplus : \mathcal{U} \times \mathcal{U} \to \mathcal{U}$ such that $(\mathcal{U}, \boxplus)$ is an abelian group;
(ii) the identity element of $(\mathcal{U}, \boxplus)$ is $\{\mathbf{0}\}$;
(iii) $X \boxplus X = \{\mathbf{0}\}$ for every group element $X \in \mathcal{U}$;
(iv) the addition operation $\boxplus$ is isometric, i.e., $d_S(X \boxplus Y_1, X \boxplus Y_2) = d_S(Y_1, Y_2)$ for all $X, Y_1, Y_2 \in \mathcal{U}$.

When a subset $\mathcal{U}$ of $\mathbb{P}_q(n)$ satisfies only the first three conditions in the above definition, it is called a *quasi-linear code*. Note that a quasi-linear code has the structure of a vector space over $\mathbb{F}_2$. As a result, the number of codewords in a quasi-linear code must be a power of 2. In fact, the following proposition was proved by Braun, Etzion and Vardy [2].

Proposition 1. *A subset $\mathcal{U} \subseteq \mathbb{P}_q(n)$, with $\{\mathbf{0}\} \in \mathcal{U}$, is a quasi-linear code if and only if $|\mathcal{U}|$ is a power of 2.*

Thus, a subspace code having a vector space structure is not very interesting by itself. It is the requirement that the addition operation $\boxplus$ be isometric that makes linear subspace codes interesting. The definition of linearity implies certain properties that an isometric linear addition must satisfy. Some of these are listed in the next three lemmas, which are taken from [2]. The first two lemmas follow easily from the definitions; for completeness, we give a proof of the third lemma.

Lemma 2. *Let $\mathcal{U}$ be a linear code in $\mathbb{P}_q(n)$ and let $\boxplus$ be the isometric linear addition on $\mathcal{U}$. Then for all $X, Y \in \mathcal{U}$, we have:*

$$\dim(X \boxplus Y) = d_S(X, Y) = \dim X + \dim Y - 2\dim(X \cap Y)$$

In particular, if $X \subseteq Y$, then $\dim(X \boxplus Y) = \dim Y - \dim X$.

Lemma 3. *For any three subspaces X, Y and Z of a linear code $\mathcal{U}$ in $\mathbb{P}_q(n)$ with isometric linear addition $\boxplus$, the condition $Z = X \boxplus Y$ implies $Y = X \boxplus Z$.*

To state the next lemma, we recall that the sum of two subspaces X and Y of $\mathbb{F}_q^n$ is defined as the subspace $X + Y = \{\mathbf{x} + \mathbf{y} : \mathbf{x} \in X, \mathbf{y} \in Y\}$.

Lemma 4. *Let $\mathcal{U}$ be a linear code in $\mathbb{P}_q(n)$ and let $\boxplus$ be the isometric linear addition on $\mathcal{U}$. If X and Y are any two codewords of $\mathcal{U}$ such that $X \cap Y = \{\mathbf{0}\}$, then $X \boxplus Y = X + Y$.*

Proof: From the definition of linearity, we have $\dim X = \dim((X \boxplus Y) \boxplus Y) = \dim(X \boxplus Y) + \dim Y - 2\dim((X \boxplus Y) \cap Y)$ and using the fact $X \cap Y = \{\mathbf{0}\}$, we also have from Lemma 2 that $\dim(X \boxplus Y) = \dim X + \dim Y$. Combining both, we obtain $\dim X = \dim X + 2\dim Y - 2\dim((X \boxplus Y) \cap Y)$, which implies $\dim Y = \dim((X \boxplus Y) \cap Y)$, i.e., $Y \subseteq (X \boxplus Y)$. Similarly, $X \subseteq (X \boxplus Y)$. This means $X + Y \subseteq X \boxplus Y$. Finally, as $X \cap Y = \{\mathbf{0}\}$, $\dim(X + Y) = \dim X + \dim Y = \dim(X \boxplus Y)$, which proves the lemma. ■

Using the above lemmas, Braun, Etzion and Vardy proved that the definition of linearity restricts the number of one-dimensional subspaces that can be included in a linear subspace code. We state their result below without proof.

Proposition 5. *Let $\mathcal{U}$ be a linear code in $\mathbb{P}_q(n)$ with isometric linear addition $\boxplus$. Then $\mathcal{U}$ contains at most n of the $q^n - 1$ one-dimensional subspaces of $\mathbb{F}_q^n$.*

Proposition 5 lends credence to the idea that a linear subspace code $\mathcal{U} \in \mathbb{P}_q(n)$ cannot have size greater than 2^n. This is because one may reasonably expect the one-dimensional codewords of $\mathcal{U}$ to form a basis of the $\mathbb{F}_2$-vector space formed by $\mathcal{U}$. Indeed, Braun, Etzion and Vardy formally conjectured that the cardinality of any linear subspace code in $\mathbb{P}_q(n)$ can be at most 2^n. They further conjectured, based on empirical evidence, that when $\mathbb{F}_q^n$ is included as a codeword, the code can contain at most $\binom{n}{k}$ k-dimensional codewords, for $0 \leq k \leq n$. The second conjecture was recently proved in [12], and is stated as a theorem below. The notation $\mathcal{U}_k$ will henceforth denote the set of all k-dimensional codewords belonging to the linear code $\mathcal{U}$, for $0 \leq k \leq n$.

Theorem 6 ([12], Theorem 2)**.** *If $\mathcal{U}$ is a linear code over $\mathbb{P}_q(n)$ that contains $\mathbb{F}_q^n$, then $|\mathcal{U}_k| \leq \binom{n}{k}$ for $0 \leq k \leq n$, and hence, $|\mathcal{U}| \leq 2^n$. Equality holds if and only if $\mathcal{U}$ is derived from a fixed basis.*

The definition of a code derived from a fixed basis is given below for easy reference.

Definition 2. *A linear subspace code $\mathcal{U}$ in $\mathbb{P}_q(n)$ is* derived from a fixed basis *if the group $(\mathcal{U}, \boxplus)$ is generated by n one-dimensional subspaces in $\mathcal{U}$.*

In this paper, we show that the Braun-Etzion-Vardy conjecture on the cardinality of linear subspace codes holds for a certain subclass of codes. This subclass is defined and characterized in the next section.

III. Linear Subspace Codes Closed under Intersection

In this section, we explore the class of linear subspace codes in $\mathbb{P}_q(n)$ that are closed under the usual set intersection operation. We start with the formal definition.

Definition 3. *A subspace code $\mathcal{U} \subseteq \mathbb{P}_q(n)$ with the property that $X \cap Y \in \mathcal{U}$ whenever $X, Y \in \mathcal{U}$ is said to be* closed under intersection.

A linear code in $\mathbb{P}_q(n)$ closed under intersection can be constructed as described in the next theorem. For a set $S \subseteq \mathbb{F}_q^n$, let $\langle S \rangle$ denote the subspace of $\mathbb{F}_q^n$ spanned by the elements of S; we specifically define $\langle \phi \rangle = \{\mathbf{0}\}$.

Theorem 7. *Let $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r\}$ be a linearly independent subset of $\mathbb{F}_q^n$ over the field $\mathbb{F}_q$ and also let $\{\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_m\}$ be a partition of $\mathcal{E}$, i.e., $\mathcal{E}_i \cap \mathcal{E}_j = \phi$ whenever $i \neq j$, $\bigcup_{i=1}^m \mathcal{E}_i = \mathcal{E}$ and $\mathcal{E}_i \neq \phi$ for $1 \leq i \leq m$. Define $\mathcal{E}_\mathcal{I} := \bigcup_{i \in \mathcal{I}} \mathcal{E}_i$ for any $\mathcal{I} \subseteq [m]$ with $\mathcal{E}_\phi := \phi$, where $[m] = \{1, 2, \ldots, m\}$. Then, $\mathcal{U} = \{\langle \mathcal{E}_\mathcal{I} \rangle : \mathcal{I} \subseteq [m]\}$ is a linear code in $\mathbb{P}_q(n)$ that is closed under intersection.*

Proof: Let us denote the symmetric difference of two sets A and B by $A \triangle B$, i.e.,

$$A \triangle B := (A \cup B) \backslash (A \cap B).$$

The operation $\triangle$ is commutative and associative.
For any two elements X and Y of $\mathcal{U}$, define the addition operation $\boxplus$ on $\mathcal{U}$ in the following way.

$$X \boxplus Y := \langle \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y} \rangle$$

where $X = \langle \mathcal{E}_{\mathcal{I}_X} \rangle$ for all $X \in \mathcal{U}$, i.e. X is the span of $\mathcal{E}_{\mathcal{I}_X}$, where $\mathcal{I}_X \subseteq [m]$ by construction. Since $\mathcal{E}$ is a linearly independent set over $\mathbb{F}_q$, choice of $\mathcal{E}_{\mathcal{I}_X}$ is unique for any $X \in \mathcal{U}$. It is obvious that $X \boxplus Y = \langle \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y} \rangle = \langle \mathcal{E}_{\mathcal{I}_X \triangle \mathcal{I}_Y} \rangle$ for all $X, Y \in \mathcal{U}$. The following points are observed.
(i) As $\phi \subset [m]$, $\langle \mathcal{E}_\phi \rangle = \langle \phi \rangle = \{\mathbf{0}\} \in \mathcal{U}$.
(ii) For any $\mathcal{I}_X, \mathcal{I}_Y \subseteq [m]$, $\mathcal{I}_X \triangle \mathcal{I}_Y$ is also a subset of $[m]$. This is because $\mathcal{E}_i$'s partition the set $\mathcal{E}$ and thus for any $\mathcal{J} \subseteq [m]$, either $\mathcal{E}_i \in \mathcal{E}_\mathcal{J}$, or $\mathcal{E}_i \cap \mathcal{E}_\mathcal{J} = \phi$. Hence $X \boxplus Y = \langle \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y} \rangle = \langle \mathcal{E}_{\mathcal{I}_X \triangle \mathcal{I}_Y} \rangle \in \mathcal{U}$ for all $X, Y \in \mathcal{U}$. Moreover, $X \boxplus Y = \langle \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y} \rangle = \langle \mathcal{E}_{\mathcal{I}_X \triangle \mathcal{I}_Y} \rangle = \langle \mathcal{E}_{\mathcal{I}_Y \triangle \mathcal{I}_X} \rangle = \langle \mathcal{E}_{\mathcal{I}_Y} \triangle \mathcal{E}_{\mathcal{I}_X} \rangle = Y \boxplus X$ for all $X, Y \in \mathcal{U}$, since $\triangle$ is commutative.
(iii) $X \boxplus X = \langle \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_X} \rangle = \{\mathbf{0}\}$ for all $X \in \mathcal{U}$, since $\mathcal{S} \triangle \mathcal{S} = \phi$.
(iv) $X \boxplus \{\mathbf{0}\} = \langle \mathcal{E}_{\mathcal{I}_X} \triangle \phi \rangle = \langle \mathcal{E}_{\mathcal{I}_X} \rangle = X$ for all $X \in \mathcal{U}$.
(v) By construction, $X \cap Y = \langle \mathcal{E}_{\mathcal{I}_X} \rangle \cap \langle \mathcal{E}_{\mathcal{I}_Y} \rangle = \langle \mathcal{E}_{\mathcal{I}_X \cap \mathcal{I}_Y} \rangle \in \mathcal{U}$ for all $X, Y \in \mathcal{U}$, since $\mathcal{I}_X \cap \mathcal{I}_Y \subseteq [m]$ for $\mathcal{I}_X, \mathcal{I}_Y \subseteq [m]$.
(vi) As $X \boxplus Y = \langle \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y} \rangle$, that means $\mathcal{E}_{\mathcal{I}_{X \boxplus Y}} = \mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y}$ for all $X, Y \in \mathcal{U}$, since any member Z of $\mathcal{U}$ is spanned by $\mathcal{E}_{\mathcal{I}_Z}$ where $\mathcal{I}_Z$ is a unique subset of $[m]$. Let $|\mathcal{E}_\mathcal{I}| := |\{j : \mathbf{e}_j \in \mathcal{E}_\mathcal{I}\}|$, then the dimension of a member X of $\mathcal{U}$ can be calculated as, $\dim X = |\mathcal{E}_{\mathcal{I}_X}|$. Now $d_S(X, Y) = \dim X + \dim Y - 2 \dim(X \cap Y) = |\mathcal{E}_{\mathcal{I}_X}| + |\mathcal{E}_{\mathcal{I}_Y}| - 2 |\mathcal{E}_{\mathcal{I}_{X \cap Y}}| = |\mathcal{E}_{\mathcal{I}_X}| + |\mathcal{E}_{\mathcal{I}_Y}| - 2 |\mathcal{E}_{\mathcal{I}_X} \cap \mathcal{E}_{\mathcal{I}_Y}| = |\mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y}|$ for all $X, Y \in \mathcal{U}$. This implies

$$\begin{aligned}
d_S(X \boxplus Z, Y \boxplus Z) &= |\mathcal{E}_{\mathcal{I}_{X \boxplus Z}} \triangle \mathcal{E}_{\mathcal{I}_{Y \boxplus Z}}| \\
&= |(\mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Z}) \triangle (\mathcal{E}_{\mathcal{I}_Y} \triangle \mathcal{E}_{\mathcal{I}_Z})| \\
&= |\mathcal{E}_{\mathcal{I}_X} \triangle (\mathcal{E}_{\mathcal{I}_Z} \triangle \mathcal{E}_{\mathcal{I}_Z}) \triangle \mathcal{E}_{\mathcal{I}_Y}| \\
&= |\mathcal{E}_{\mathcal{I}_X} \triangle \phi \triangle \mathcal{E}_{\mathcal{I}_Y}| \\
&= |\mathcal{E}_{\mathcal{I}_X} \triangle \mathcal{E}_{\mathcal{I}_Y}| \\
&= d_S(X, Y)
\end{aligned}$$

for all $X, Y, Z \in \mathcal{U}$.
(i) proves the existence of $\{\mathbf{0}\}$ in the structure. (ii) establishes that $\{\mathcal{U}, \boxplus\}$ is an abelian group. (iii) and (iv) prove idempotency and additive inverse of that group respectively. (v) shows that the code is closed under intersection. Finally (vi) accounts for translation invariance in the structure, thus proving that $\mathcal{U}$ is a linear code in $\mathbb{P}_q(n)$ that is closed under intersection. ■

Theorem 7 gives us a systematic method of constructing linear subspace codes that are closed under intersection. A code constructed in this manner will be referred to as a *code derived from a partition of a linearly independent set.* As stated in Theorem 8 below, this is in fact the *only* means of constructing linear subspace codes closed under intersection.

Theorem 8. *Let $\mathcal{U}$ be a linear subspace code that is closed under intersection. Then, there exist a set of linearly independent vectors $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r\}$ and a partition $\{\mathcal{E}_1, \mathcal{E}_2, \ldots, \mathcal{E}_m\}$ of $\mathcal{E}$ such that $\mathcal{U} = \{\langle \mathcal{E}_\mathcal{I} \rangle : \mathcal{I} \subseteq [m]\}$.*

Theorems 7 and 8 together give a characterization of the class of linear subspace codes that are closed under intersection. Our proof of Theorem 8 requires the notion of indecomposable codewords, which we define next.

Definition 4. *A codeword $Y \neq \{\mathbf{0}\}$ of a linear subspace code $\mathcal{U}$ is said to be* indecomposable *if Y cannot be expressed as $Y_1 \boxplus Y_2$ for any $Y_1, Y_2 \in \mathcal{U}$ with $\dim Y_1, \dim Y_2 < \dim Y$.*

The next few lemmas record some important properties of indecomposable codewords that we will use in our proof of Theorem 8.

Lemma 9. *Let Y be an indecomposable codeword of a linear subspace code $\mathcal{U}$. Then, for any codeword $X \in \mathcal{U}$, we have $X \subseteq Y$ iff $X = \{\mathbf{0}\}$ or $X = Y$.*

Proof: Suppose that $X \subset Y$ for some X with $0 < \dim X < \dim Y$. Then, we also have $\dim(X \boxplus Y) = \dim Y - \dim X < \dim Y$. Since we can always write $Y = X \boxplus (X \boxplus Y)$, this means that Y cannot be indecomposable. ■

Lemma 10. *If Y_1, Y_2 are any two distinct indecomposable codewords of a linear subspace code $\mathcal{U}$ that is closed under intersection, then $Y_1 \cap Y_2 = \{\mathbf{0}\}$. Consequently, $Y_1 \boxplus Y_2 = Y_1 + Y_2$, and $\dim(Y_1 \boxplus Y_2) = \dim Y_1 + \dim Y_2$.*

Proof: Consider any indecomposable $Y_1, Y_2 \in \mathcal{U}$ with $Y_1 \neq Y_2$. Obviously $Y_1 \cap Y_2 \in \mathcal{U}$. By Lemma 9, we cannot have $Y_1 \subset Y_2$, and so $\dim(Y_1 \cap Y_2) < \dim(Y_1)$. Since $Y_1 \cap Y_2 \subset Y_1$, we must have $Y_1 \cap Y_2 = \{\mathbf{0}\}$ by Lemma 9 again. The facts about $Y_1 \boxplus Y_2$ now follow from Lemma 4. ■

The following generalization of Lemma 10 plays a key role in our proof of Theorem 8.

Lemma 11. *Let $Y_1, Y_2, \ldots, Y_m$, $m \geq 2$, be distinct indecomposable codewords of a linear subspace code $\mathcal{U}$ that is closed under intersection. Then,*

(a) *for all $j \in [m]$, $Y_j \cap \sum_{i \in [m] \setminus \{j\}} Y_i = \{\mathbf{0}\}$;*
(b) *$Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m = Y_1 + Y_2 + \cdots + Y_m$; and*
(c) *$\dim(Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m) = \sum_{i=1}^{m} \dim(Y_i)$.*

Proof: We prove (a)–(c) simultaneously by induction on the number of indecomposable codewords. The base case of two codewords is covered by Lemma 10. As the induction hypothesis, assume that the statements (a)–(c) hold for any set of $m-1$ indecomposable codewords, for some $m \geq 3$. In particular, for any $(m-1)$-subset $\mathcal{I} \subset [m]$, we have $\boxplus_{i \in \mathcal{I}} Y_i = \sum_{i \in \mathcal{I}} Y_i$ and $\dim(\boxplus_{i \in \mathcal{I}} Y_i) = \sum_{i \in \mathcal{I}} \dim Y_i$.

Now, suppose that (a) does not hold for the given set of m indecomposable codewords $Y_1, Y_2, \ldots, Y_m$. Without loss of generality, assume that $Y' := Y_m \cap (Y_1 + \cdots + Y_{m-1}) \neq \{\mathbf{0}\}$. By the induction hypothesis, $Y_1 + \cdots + Y_{m-1} = Y_1 \boxplus \cdots \boxplus Y_{m-1}$ is in $\mathcal{U}$, and hence, so is Y'. Since $Y' \subseteq Y_m$, we have $Y' = Y_m$ by Lemma 9. Thus, $Y_m \subset Y_1 + \cdots + Y_{m-1}$. This further implies that $Y_2 + \cdots + Y_{m-1} + Y_m \subseteq Y_1 + \cdots + Y_{m-1}$. By the induction hypothesis, this is equivalent to $(Y_2 \boxplus \cdots \boxplus Y_m) \subseteq (Y_1 \boxplus \cdots \boxplus Y_{m-1})$.

Now, consider $Z = (Y_1 \boxplus \cdots \boxplus Y_{m-1}) \boxplus (Y_2 \boxplus \cdots \boxplus Y_m)$. On the one hand, we have $\dim Z = \dim(Y_1 \boxplus \cdots \boxplus Y_{m-1}) - \dim(Y_2 \boxplus \cdots \boxplus Y_m)$ by Lemma 2, and hence, applying the induction hypothesis,

$$\dim Z = \sum_{i=1}^{m-1} \dim Y_i - \sum_{i=2}^{m} \dim Y_i = \dim Y_1 - \dim Y_m. \quad (1)$$

On the other hand, $Z = Y_1 \boxplus Y_m$, so that by Lemma 10, $\dim Z = \dim Y_1 + \dim Y_m$, which contradicts (1) since $\dim Y_m \neq 0$. Hence, (a) must hold for $Y_1, Y_2, \ldots, Y_m$.

The statements (b) and (c) follow easily from (a) by induction using Lemma 4. ■

We are now in a position to prove Theorem 8.

Proof of Theorem 8: Let $Y_1, \ldots, Y_m$ be a listing of all the distinct indecomposable codewords of $\mathcal{U}$. For each $i \in [m]$, fix a basis $\mathcal{E}_i$ of Y_i. It follows from Lemma 11(a) that $\mathcal{E} = \bigcup_{i=1}^{m} \mathcal{E}_i$ is a linearly independent subset of $\mathbb{F}_q^n$, and that $\{\mathcal{E}_1, \ldots, \mathcal{E}_m\}$ constitutes a partition of $\mathcal{E}$. As a consequence, for any $\mathcal{I} \subseteq [m]$, we have $\langle \mathcal{E}_{\mathcal{I}} \rangle = \sum_{i \in \mathcal{I}} Y_i = \boxplus_{i \in \mathcal{I}} Y_i$, the last equality being due to Lemma 11(b). Thus, $\langle \mathcal{E}_{\mathcal{I}} \rangle \in \mathcal{U}$ for all $\mathcal{I} \subseteq [m]$.

To complete the proof, we must show that any codeword $X \in \mathcal{U}$ is of the form $\langle \mathcal{E}_{\mathcal{I}} \rangle$ for some $\mathcal{I} \subseteq [m]$. This is trivially true if $X = Y_i$ for some $i \in [m]$. So suppose that X is not indecomposable. Then, it can be decomposed into a sum of the form $X_1 \boxplus X_2$ with $\dim X_1, \dim X_2 < \dim X$. Now, X_1 and X_2 are either indecomposable or can be further decomposed. Carrying on in this manner, X can be decomposed into a sum of the form $\boxplus_{i \in \mathcal{I}} Y_i$. Hence, $X = \langle \mathcal{E}_{\mathcal{I}} \rangle$ for some $\mathcal{I} \subseteq [m]$, which completes the proof. ■

The proof above used the fact that any codeword $X \in \mathcal{U}$ could be decomposed into a sum of the form $\boxplus_{i \in \mathcal{I}} Y_i$. Such a decomposition is, in fact, unique.

Proposition 12. *Let $\mathcal{U}$ be a linear subspace code that is closed under intersection, and let $Y_1, Y_2, \ldots, Y_m$ be its indecomposable codewords. Then, any codeword $X \in \mathcal{U}$ can be uniquely expressed as $\boxplus_{i \in \mathcal{I}} Y_i$ for some $\mathcal{I} \subseteq [m]$.*

Proof: Suppose that $X \in \mathcal{U}$ can be expressed as $\boxplus$ of indecomposable codewords in two different ways:

$$X = \boxplus_{i \in \mathcal{I}} Y_i = \boxplus_{j \in \mathcal{J}} Y_j$$

for distinct subsets $\mathcal{I}$ and $\mathcal{J}$ of $[m]$. Then, upon some reorganization and possible cancellation of like terms, we would obtain for some $i \in \mathcal{I} \cup \mathcal{J}$ and some $\mathcal{L} \subseteq [m] \setminus \{i\}$, $Y_i = \boxplus_{\ell \in \mathcal{L}} Y_\ell$. By Lemma 11(b), this is the same as $Y_i = \sum_{\ell \in \mathcal{L}} Y_\ell$, which contradicts Lemma 11(a). ■

From the proof of Theorem 8 (and the statement of Proposition 12), it is clear that any linear subspace code closed under intersection is generated by its indecomposable codewords. This motivates the following definition.

Definition 5. *The* generating set, *$\mathcal{U}_G$, of a linear subspace code $\mathcal{U}$ closed under intersection is the set of all its indecomposable codewords.*

Note that any one-dimensional codeword of $\mathcal{U}$ is indecomposable, and hence is in the generating set. More generally, we have the following strengthening of Lemma 9.

Lemma 13. *Let $\mathcal{U}$ be a linear subspace code closed under intersection. For any $Y \in \mathcal{U}$, we have $Y \in \mathcal{U}_G$ if and only if there is no $X \in \mathcal{U}$, $X \neq \{\mathbf{0}\}$, such that $X \subset Y$.*

Proof: The "only if" part holds by Lemma 9. For the "if" part, assume that $Y \in \mathcal{U}$ is such that for all $X \in \mathcal{U}$, $X \subset Y$ implies $X = \{\mathbf{0}\}$. If $Y \notin \mathcal{U}_G$, then by Proposition 12, Y can be expressed as $\boxplus_{i=1}^{r} Y_i$ for some indecomposable codewords $Y_1, \ldots, Y_r$. Evidently $r \geq 2$, otherwise Y would itself be in $\mathcal{U}_G$. Therefore, by Lemma 11(b), we have $Y = \sum_{i=1}^{r} Y_i$, which means $Y_i \subset Y$ for $1 \leq i \leq r$, $r \geq 2$. Hence, proved by contradiction. ■

The following property of generating sets will be useful in the next section.

Lemma 14. *Let $\mathcal{U}$ and $\mathcal{V}$ be two linear subspace codes, each closed under intersection. If $\mathcal{U}_G \subset \mathcal{V}_G$, then $\mathcal{U} \subset \mathcal{V}$.*

Proof: Obviously, if $\mathcal{U}_G \subseteq \mathcal{V}_G$, then $\mathcal{U} \subseteq \mathcal{V}$. Moreover, $\mathcal{U}_G = \mathcal{V}_G$ iff $\mathcal{U} = \mathcal{V}$. ■

Remark 1. *The converse statement of Lemma 14, namely, that $\mathcal{U} \subset \mathcal{V}$ implies $\mathcal{U}_G \subset \mathcal{V}_G$, is not true in general. For example, let $\{\mathbf{e}_1, \mathbf{e}_2\}$ be a basis for $\mathbb{F}_q^2$, and consider $\mathcal{U}_G = \{\langle \mathbf{e}_1, \mathbf{e}_2 \rangle\}$*

and $\mathcal{V}_G = \{\langle \mathrm{e}_1 \rangle, \langle \mathrm{e}_2 \rangle\}$.

We end this section by noting that codes derived from a fixed basis (see Definition 2) form a special case of codes derived from partitions of linearly independent sets. This connection will be explored further in the next section.

IV. Maximality of Linear Subspace Codes Closed under Intersection

In this section, we prove the conjecture of Braun, Etzion and Vardy [2] for the class of linear subspace codes that are closed under intersection. We also identify the maximal linear subspace codes under the constraint of closure under intersection.

Definition 6. *A linear code $\mathcal{U}$ closed under intersection in $\mathbb{P}_q(n)$ is said to be maximal if and only if for any other linear code $\mathcal{V}$ closed under intersection, $\mathcal{U} \subseteq \mathcal{V} \Rightarrow \mathcal{U} = \mathcal{V}$.*

We start with a small observation on the dimensions of the indecomposable codewords of any linear subspace code closed under intersection.

Lemma 15. *If $\mathcal{U}$ is a linear code closed under intersection in $\mathbb{P}_q(n)$ with generating set $\mathcal{U}_G = \{Y_1, Y_2, \ldots, Y_m\}$, then $\sum_{i=1}^m \dim Y_i \leq n$.*

Proof: By Proposition 12, the maximum dimension of a codeword in $\mathcal{U}$ is $\dim(Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m)$, which equals $\dim(\sum_{i=1}^m Y_i)$ by Lemma 11. The last sum cannot exceed n since $\mathcal{U} \subset \mathbb{P}_q(n)$, and the lemma is proved. ■

The following result is concerned with the maximality of linear subspace codes closed under intersection.

Proposition 16. *Let $\mathcal{U}$ be a linear subspace code closed under intersection in $\mathbb{P}_q(n)$ with generating set $\mathcal{U}_G = \{Y_1, Y_2, \ldots, Y_m\}$. Then $\mathcal{U}$ is maximal only if $\sum_{i=1}^m \dim Y_i = n$.*

Proof: We will show that if $\sum_{i=1}^m \dim Y_i = s < n$, then $\mathcal{U}$ cannot be maximal. By Lemma 11, we have $\dim(Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m) = \sum_{i=1}^m \dim Y_i = s$. Any bases for the Y_is when combined together will form a basis for $\mathbb{F}_q^s$. This can be extended to a basis of $\mathbb{F}_q^n$ by adding $n-s$ more vectors, say $\{x_1, x_2, \ldots, x_{n-s}\}$, where $x_j \in \mathbb{F}_q^n$ for all $1 \leq j \leq (n-s)$. Consider $X = \langle x_1, x_2, \ldots, x_{n-s} \rangle$. If X is added to the generating set $\mathcal{U}_G$ then by Definition 5 and Proposition 12, $\mathcal{V}_G = \{X, Y_1, Y_2, \ldots, Y_m\} \supset \mathcal{U}_G$ is the generating set for another linear subspace code $\mathcal{V}$ closed under intersection. By Lemma 14, $\mathcal{U}$ cannot be maximal.

Thus, if $\mathcal{U}$ is maximal, then by Lemma 15, $\sum_{i=1}^m \dim Y_i = n$. ■

When a linear subspace code closed under intersection is maximal, it is natural to ask what other constraints are imposed on its structure. The next lemma will give us some answer to this question.

Corollary 16.1. *Let $\mathcal{U}$ be a linear subspace code closed under intersection in $\mathbb{P}_q(n)$. Then $\mathcal{U}$ is maximal only if $\mathbb{F}_q^n \in \mathcal{U}$.*

Proof: Suppose $\mathcal{U}$ is maximal. If $\mathcal{U}_G = \{Y_1, Y_2, \ldots, Y_m\}$ be its generating set then by Proposition 16, $\dim(Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m) = \sum_{i=1}^m \dim Y_i = n$ and hence, $Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m = \mathbb{F}_q^n \in \mathcal{U}$. ■

Let us now prove the conjecture of Braun, Etzion and Vardy for the class of linear subspace codes closed under intersection.

Proposition 17. *The size of the largest linear subspace code in $\mathbb{P}_q(n)$ that is closed under intersection is 2^n.*

Proof: If $\mathcal{U}$ is a linear subspace code closed under intersection with $Y_1, Y_2, \ldots, Y_m$ being the only indecomposable codewords of $\mathcal{U}$, then according to Lemma 11, $\dim(Y_1 \boxplus Y_2 \boxplus \cdots \boxplus Y_m) = \dim(Y_1 + Y_2 + \cdots + Y_m) = \sum_{i=1}^m \dim Y_i \geq m$ and by Lemma 15, $\sum_{i=1}^m \dim Y_i \leq n$. Combining both gives $m \leq n$. Again Proposition 12 states that a codeword of $\mathcal{U}$ can be achieved as $\boxplus$ of some or all of $Y_1, Y_2, \ldots, Y_m$ in a unique way. Since the total number of all such possible combinations of Y_i's is 2^m, it readily follows that $|\mathcal{U}| = 2^m \leq 2^n$. ■

Corollary 17.1. *Let $\mathcal{U}$ be a linear subspace code in $\mathbb{P}_q(n)$ closed under intersection such that $|\mathcal{U}| = 2^n$. Then $\mathbb{F}_q^n \in \mathcal{U}$. Furthermore, $|\mathcal{U}_G| = n$ and $\dim Y = 1$ for all $Y \in \mathcal{U}_G$.*

Proof: The fact that $\mathbb{F}_q^n \in \mathcal{U}$ follows directly from Proposition 17 and Corollary 16.1. Using the existence of $\mathbb{F}_q^n$, it also follows from Theorem 6 that $|\mathcal{U}_1| = n$, thus $|\mathcal{U}_G| \geq n$. Finally using Lemma 15, we get the rest. ■

The following result reveals that only the codes derived from a fixed basis can have the maximum cardinality among the class of linear subspace codes closed under intersection.

Lemma 18. *If $\mathcal{U}$ is a linear subspace code in $\mathbb{P}_q(n)$ closed under intersection, then the size of $\mathcal{U}$ is 2^n if and only if $\mathcal{U}$ is a code derived from a fixed basis.*

Proof: If $|\mathcal{U}| = 2^n$, then $\mathcal{U}$ is derived from a fixed basis follows from Theorem 6 and Corollary 17.1.

Conversely, let $\mathcal{U}$ be a code derived from a fixed basis, then according to Definition 2, $|\mathcal{U}_1| = n$. That means $\mathcal{U}_G = \mathcal{U}_1$ by Lemma 15 and hence $|\mathcal{U}| = 2^n$. ■

We conclude this section with the following result which identifies only those linear codes that can attain maximality when subjected to closure under intersection.

Proposition 19. *Let $\mathcal{U}$ be a linear subspace code in $\mathbb{P}_q(n)$ closed under intersection. Then $\mathcal{U}$ is maximal if and only if $\mathcal{U}$ is derived from a fixed basis.*

Proof: If $\mathcal{U}$ is a code which is derived from a fixed basis, then by Lemma 18 and Proposition 17, $|\mathcal{U}| = 2^n$, and therefore it is maximal.

Conversely, assume $\mathcal{U}$ to be a maximal linear code closed under intersection which is not derived from a fixed basis. According to Corollary 16.1, $\mathbb{F}_q^n \in \mathcal{U}$ and using Theorem 6 as well as Definition 2, $|\mathcal{U}_1| < n$, which means $\mathcal{U}_G \supset \mathcal{U}_1$ by Proposition 16. There must exist some $Y \in \mathcal{U}_G$ such that $Y \notin \mathcal{U}_1$, since $\mathcal{U}_G \backslash \mathcal{U}_1 \neq \phi$. Pick any basis $\mathcal{B}_Y$ for Y. If $\mathcal{B}_Y = \{\mathrm{e}_1, \mathrm{e}_2, \ldots, \mathrm{e}_{\dim Y}\}$, then consider the linear code $\mathcal{W}$ closed under intersection and characterized by $\mathcal{W}_G = \{\mathcal{U}_G \backslash Y\} \cup$

$\{\langle \mathbf{e}_j \rangle\}_{j=1}^{\dim Y}$. Evidently $\langle \mathbf{e}_j \rangle \notin \mathcal{U}$ by Lemma 13 for all $1 \leq j \leq \dim Y$. On the other hand $Y \in \mathcal{W}$ although $Y \notin \mathcal{W}_G$. Hence, $\mathcal{W} \supset \mathcal{U}$, a contradiction to our initial assumption. Therefore, proved. ■

V. Conclusion

In this paper, we introduced the class of linear subspace codes closed under intersection. We characterized this class of codes in terms of partitions of linearly independent subsets of $\mathbb{F}_q^n$. We also proved that a linear code closed under intersection is maximal if and only if it is derived from a fixed basis.

The conjecture by Braun, Etzion and Vardy [2] on the maximum cardinality of a linear subspace code was shown to be true for the particular case of linear codes closed under intersection. However, the general conjecture that any linear subspace code has a maximum cardinality of 2^n is yet to be resolved and would be an interesting problem for future research.

References

[1] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, pp. 3579–3591, Aug. 2008.

[2] M. Braun, T. Etzion and A. Vardy, "Linearity and complements in projective space," *Linear Algebra and Its Applications*, vol. 438, no. 1, pp. 57–70, 2013.

[3] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Trans. Inform. Theory*, vol. 57, pp. 1165–1173, Feb. 2011.

[4] T. Etzion and N. Silberstein, "Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams," *IEEE Trans. Inform. Theory*, vol. 55, pp. 2909–2919, July 2009.

[5] N. Silberstein and T. Etzion, "Enumerative coding for Grassmannian space," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 365–374, January 2011.

[6] M. Gadouleau and Z. Yan, "Packing and covering properties of subspace codes for error control in random linear network coding," *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2097–2108, May 2010.

[7] A-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, "Cyclic orbit codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7386–7404, Nov. 2013.

[8] S.T. Xia and F.W. Fu, "Johnson type bounds on constant dimension codes," *Designs, Codes, Crypto.*, vol. 50, pp. 163–172, 2009.

[9] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," *Lecture Notes in Computer Science*, vol. 5393, pp. 31–42, 2008.

[10] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3207–3216, July 2010.

[11] S.B. Pai and B.S. Rajan, "A lattice Singleton bound," *Proc. 2013 IEEE Int. Symp. Inf. Theory (ISIT 2013)*, pp. 1904–1908.

[12] S.B. Pai and B.S. Rajan, "On the bounds of certain maximal linear codes in a projective space," *ArXiv:1410.2725*.

[13] F.J. Macwilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publishing Co., 1977.

[14] L. Lovasz, "Flats in matroids and geometric graphs," *Combinatorial Surveys: Proceedings of the Sixth British Combinatorial Conference*, pp. 45–86, 1977.