A Lattice Singleton Bound

Srikanth B. Pai and B. Sundar Rajan  
Dept. of ECE, Indian Institute of Science,  
Bangalore 560012, India  
Email:{spai,bsrajan}@ece.iisc.ernet.in

Abstract—The binary coding theory and subspace codes for random network coding exhibit similar structures. The method used to obtain a Singleton bound for subspace codes mimic the technique used in obtaining the Singleton bound for binary codes. This motivates the question of whether there is an abstract framework that captures these similarities. As a first step towards answering this question, we use the lattice framework proposed in [1]. A lattice is a partially ordered set in which any two elements have a least upper bound and a greatest lower bound. A ‘lattice scheme’ is defined as a subset of a lattice. In this paper, we derive a Singleton bound for lattice schemes and obtain Singleton bounds known for binary codes and subspace codes as special cases. The lattice framework gives additional insights into the bounds known for binary codes and subspace codes. We also obtain a new upper bound on the code size for non-constant dimension codes. The plots of this bound along with plots of the code sizes of known non-constant dimension codes in the literature reveal that our bound is tight for certain parameters of the code.

I. INTRODUCTION AND BACKGROUND

In the field of coding theory, calculations of good upper and lower bounds on the size of a code serves as a benchmark for code design. Techniques of constructing subspace codes for error correction in random network coding (also called ‘projective space codes’) are similar to the techniques used to construct binary codes. A projective space code is defined as a subset of subspaces of a vector space. The viewpoint of lattice theory for projective space codes has already been suggested [2], [3], [4]. A lattice is a partially ordered set in which any two elements have a least upper bound and a greatest lower bound. The set of all subspaces of a vector space is a lattice. The set of all subsets of a set is called a power set. Both the power set and the projective space form lattices under inclusion order. A ‘lattice scheme’ is defined as a subset of a lattice. It has already been observed in [1] that binary codes and projective space codes are lattice schemes. Binary codes are power set schemes and projective space codes are projective space schemes. The lattice framework common to projective space codes and binary codes have also been observed in [3] and [4]. The authors of [4] establish that the projective space codes are analogs of classical binary codes. They also investigate the notions of linearity and complements of a code. In [1], the relationship between binary codes and projective space codes is investigated thoroughly using the framework of lattices and a generalized notion of orthogonal complement is introduced for lattices.

One of the ways to generate a bound on the code size is to capture a bare minimum structure for the bound through an appropriate mathematical abstraction and generalize the approach. For example, the introduction of ‘Association Schemes’ captured the notion of sphere packing and sphere covering arguments in traditional coding theory [5] and strengthened the bounds by a linear programming approach. In our paper, the notion of Singleton bound is generalized using the framework of lattices. Since error correcting codes for random network coding was proposed in [2], there has been a lot of activity in the theory of projective space codes. The authors of [2] consider projective space codes in which all the subspaces are of the same dimension. Such codes are called constant dimension codes. The Koetter-Kschischang Singleton bound (KKS bound) for constant dimension codes was derived and achieved asymptotically in [2].

In the case of binary codes, Hamming distance between two binary vectors is a metric on the binary coding space. Similarly the subspace distance, introduced in [2], between two subspaces of a vector space is a metric on the projective space. In a projective space, the number of elements in a sphere of a particular radius depends on the center of that sphere [2]. However, in the case of binary codes, the number of elements in a sphere depends only on the radius of the sphere and not on the center of the sphere. So the subspace distance on the projective space behaves differently from the Hamming distance on the usual binary vectors. As noted in [6], the anticode bound introduced in [5] gives a setting in which one can get tighter sphere packing bounds for constant dimension codes. A close look at the bounds for subspace distance and non-existence of nontrivial perfect codes has been given in [6]. An appropriate generalization for Singleton bounds (analogous to association scheme for sphere packing/covering bounds) is not known yet. In this paper, we propose that the lattice framework is appropriate for generalizing Singleton bounds. We derive an upper bound on the size of a lattice scheme, which will be called Lattice Singleton Bound (LSB) for the remainder of the paper. We get the KKS bound and the classical Singleton bound as special cases of the LSB.

While most results in projective space codes assume that the dimensions of the subspaces in the code are constant, a few papers in literature have considered codes with non-constant dimension. In particular, the authors of [6] derive a Gilbert-Varshamov type bound, which we will term as ‘Etzion Vardy- Gilbert Varshamov Bound’ (EV-GVB), for non-constant dimension codes. We derive a new upper bound on the code size for non-constant dimension codes by applying the LSB to the projective lattice. To the best of our knowledge,
our Singleton bound is the first upper bound for non-constant dimension codes.

The construction of constant dimension codes have been the main focus in the field of code constructions for projective spaces. The first constant dimension subspace codes introduced in [2] achieve the KKS bound asymptotically. And there is no known code constructions that exactly achieve the Singleton bound proposed in [2], [6]. The question of achieving that Singleton bound is an open question. A large class of constant and non-constant dimension codes using Ferrer’s diagrams and Lifted Rank Metric codes are constructed in [7], [8], [9]. The authors of [10] report marginal improvements over the size of the code compared to the codes of [7]. A plot of code sizes of the codes reported in [10], [7] compared to a plot of our upper bound with a Gilbert-Varshamov type lower bound. The code size with the code sizes of non-constant dimension codes found in the literature. We also compare our upper bound to the codes of [7]. A plot of code sizes of the code compared to the codes of [7].

IV introduces the Singleton bound in the framework of lattice codes and subspace codes are both lattice schemes. Section V of the paper is organized as follows: We introduce the preliminaries of lattices in Section II. Section III introduces the idea of lattice schemes where it is shown that classical codes and subspace codes are both lattice schemes. Section IV introduces the Singleton bound in the framework of lattice schemes and contains the main theorem of this paper. Section V contains the main distinguishing feature of projective space codes which we believe make Singleton type bounds weak in projective spaces. In Section V, we obtain a new upper bound for non-constant dimension codes and plot our upper bound with EV-GVB along with different codes constructed in the literature. Finally, in Section VI we conclude by summarizing our contributions and discussing the scope for future work.

Notations: A set is denoted by a capital letter and its elements will be denoted by small letters (For example, \( x \)). We will assume, for the purposes of the paper, that all the lattices are finite and have a unique greatest element denoted by \( \oplus \), and a unique least element denoted by \( \ominus \).

Definition 1: A poset is a pair \((P, \leq)\), where \( P \) is a set and \( \leq \) is a binary relation (called the order relation) on the set \( P \) satisfying:

1) (Reflexivity) For all \( x, x \leq x \).
2) (Antisymmetry) If \( x \leq y, y \leq x \), then \( x = y \).
3) (Transitivity) If \( x \leq y, y \leq z \), then \( x \leq z \).

For the remainder of the paper, \( P \) denotes a poset with \( \leq \) as the order relation. If \( x \leq y \) and \( x \neq y \), then we use the shorthand \( x < y \). \( x \leq y \) is read as "\( x \) is less than \( y \)" or "\( x \) is contained in \( y \)."

Definition 2: An upper bound (lower bound) of a subset \( X \) of \( P \) is an element \( a \in P \) containing (contained in) every \( x \in X \). The least upper bound (greatest lower bound) of \( X \) is the element of \( P \) contained in (containing) every upper bound (lower bound) of \( X \).

If a least upper bound, or a greatest lower bound of a set exists, it is unique due to the antisymmetry property of the order relation (Definition 1). The least upper bound of a set \( X \) is denoted by \( \sup X \) and the greatest lower bound is denoted by \( \inf X \).

Definition 3: A lattice \( L \) is a poset which has the property that \( \forall a, b \in L \), the sup\( \{a, b\} \) exists and inf\( \{a, b\} \) exists. The sup\( \{a, b\} \) is denoted by \( a \lor b \) (read as "\( a \) join \( b \)") and the inf\( \{a, b\} \) is denoted by \( a \land b \) (read as "\( a \) meet \( b \)").

Definition 4: A sublattice of a lattice \( L \) is a subset \( K \) of \( L \) that satisfies the following condition:

\[
\begin{align*}
  a, b &\in K \implies a \lor b \in K, a \land b \in K
\end{align*}
\]

Definition 5: A map \( \psi \) from \( L \) to \( K \) is said to be a lattice homomorphism if it satisfies the following conditions:

1) \( \psi(a \lor b) = \psi(a) \lor \psi(b) \)
2) \( \psi(a \land b) = \psi(a) \land \psi(b) \)
Further, if \( \psi \) is bijective, then we say that \( L \) and \( K \) are isomorphic.

**Example 1:** Let \( X = \{1, 2, 3\} \) and \( \mathcal{P}(X) \) denote the power set of \( X \). We can view \( (\mathcal{P}(X), \subseteq) \) as a poset where set inclusion is the order relation. The power set under this order is a lattice. For any subsets \( A \) and \( B \), \( A \cup B = \overline{A \cap B} \) and \( A \cap B = A \cap B \). Further, the lattice generated by subsets of \( \{1, 2\} \) is a sublattice. Notice that \( I = X \) and \( O = \emptyset \). □

One can completely specify an order of a poset (finite ones) by a Hasse diagram, like the one shown in Fig. 1. If \( a \leq b \) and there is no \( t \) such that \( a \leq t \leq b \), we say that “\( b \) covers \( a \)”. In the Hasse diagram of a lattice, \( a \) and \( b \) are joined iff \( b \) covers \( a \) or \( a \) covers \( b \). The diagram is drawn in such a way that if \( b \) covers \( a \), then \( b \) is written above \( a \). Clearly, \( a \leq b \) iff there exists a path from \( a \) moving up to \( b \). The order relation is completely specified by such a diagram. Naturally, \( I \) will be the topmost element and \( O \) will be the lowest element.

For a set \( X \), \( (\mathcal{P}(X), \cup, \cap) \) will denote lattice of the power set of \( X \) with union and intersection as join and meet of the lattice respectively.

**Definition 6:** A lattice \( (L, \lor, \land) \) is distributive if the following conditions hold:

1. For all \( a, b, c \in L \), \( a \lor (b \land c) = (a \lor b) \land (a \lor c) \).
2. For all \( a, b, c \in L \), \( a \land (b \lor c) = (a \land b) \lor (a \land c) \).

It is immediate that for any set \( X \), \( (\mathcal{P}(X), \cup, \cap) \) is a distributive lattice. However all lattices are not distributive, as seen in the examples below.

**Example 2:** Let \( V \) be a vector space of dimension \( n \) over a field \( \mathbb{F}_q \). The class of all the subspaces of \( V \), denoted by \( \text{Sub}(V) \), can be ordered under inclusion in a manner similar to a set. The join of two subspaces \( A \) and \( B \) will then be the smallest subspace containing both \( A \) and \( B \). This means that \( A \lor B = A + B \) and the largest subspace contained in both \( A \) and \( B \) is \( A \land B \). So the meet of \( A \) and \( B \) is \( A \land B \). A such lattice will be denoted as \( (\text{Sub}(V), +, \cap) \). Clearly \( I = V \) and \( O = \{0\} \). This lattice will be called the projective lattice.

This lattice is not distributive. To see this, we consider the vector space \( V = \mathbb{F}_2^{3} \) over \( \mathbb{F}_2 \).

The Hasse diagram of \( (\text{Sub}(\mathbb{F}_2^{3}), +, \cap) \) is shown in Fig. 2.

Here, \( A = \{(0, 1)\} \), \( B = \{(1, 0)\} \) and \( C = \{(1, 1)\} \).

Clearly,

\[
A \lor (B \land C) = A \lor B + A \land C = \{(0, 0)\}
\]

and thus \( (\text{Sub}(\mathbb{F}_2^{3}), +, \cap) \) is not distributive. \( (\text{Sub}(\mathbb{F}_2^{3}), +, \cap) \) is identified by the name \( M_3 \). □

The above lattice is not distributive, i.e. \( A \lor (B \land C) = A \lor B + A \land C \) fails for three distinct subspaces \( A, B, C \) if \( A \subseteq C \), one can prove that \( A \lor (B \land C) = (A + B) \land C \) and thus it behaves partly distributively. This property is captured in the following definition:

**Definition 7:** A lattice \( (L, \lor, \land) \) is modular if the following condition holds:

- (Modularity) If \( a \leq c \), then \( a \lor (b \land c) = (a \lor b) \land c \).

If the lattice is distributive, the modularity condition holds. This means that any distributive lattice is modular. However \( (\text{Sub}(V), +, \cap) \) is a modular lattice that is non distributive.

The observation that for \( (\text{Sub}(V), \cup, \cap) \), any two elements \( A, B \) satisfy \( |A \cup B| + |A \cap B| = |A| + |B| \), and in an analogous fashion, for \( (\text{Sub}(V), +, \cap) \), any two elements \( A, B \) satisfy \( \dim(A + B) + \dim(A \cap B) = \dim(A) + \dim(B) \), seems to suggest that modular lattices must satisfy an equation of the form \( v(a \lor b) + v(a \land b) = v(a) + v(b) \) for some real-valued function \( v \) on the lattice. This is indeed true and in turn, such a function helps characterise modular lattices. We need the following few definitions and results to make the characterisation precise.

**Definition 8:** An isotone valuation on a lattice \( L \) is a real valued function \( v \) on \( L \) that satisfies:

1. (Valuation) For all \( x, y \in L \),
   \[
   v(x \lor y) + v(x \land y) = v(x) + v(y).
   \]
2. (Isotone) \( x \leq y \implies v(x) \leq v(y) \)

Additionally, the isotone valuation is called positive, if \( x < y \implies v(x) < v(y) \).

**Theorem 1:** [11, pg.230, Th.1] Given a lattice \( L \) and an isotone valuation \( v \), the function \( d_v(a, b) := v(a \lor b) - v(a \land b) \) is a metric iff \( v \) is positive. In general, \( d_v \) is a pseudo metric.

In a lattice \( (L, \lor, \land) \), a chain \( C \) is a subset of \( L \) with the property that for all \( a, b \in C \), \( a \leq b \) or \( b \leq a \). We say that in a chain, any two elements are comparable. Given two elements
Fig. 3. The $N_5$ lattice: A lattice without Jordan-Dedekind property

Fig. 4. Two non-geometric lattices: In part (A), a non-geometric distributive lattice $L_1$ is shown. In part (B), a non-geometric, non-distributive modular lattice $L_2$ is depicted.

$a, b \in L$, a chain $\{x_1, x_2, \ldots, x_l\}$ of $L$ with the property $a = x_0 < x_1 < \cdots < x_l = b$ is called a chain between $a$ and $b$. The length of the chain is defined as $l$.

Definition 9: The height of an element $x$ in a lattice $L$ is the maximum length of a chain between $O$ and $x$. It is denoted by $h_L(x)$.

The number $h_L(I)$ is called the height of the lattice $L$ or the dimension of $L$. Note that the chain from $O$ to $O$ contains only one element, and thus $h_L(O) = 0$. We need an additional property to characterise modular lattices.

Definition 10: A lattice is said to have the Jordan-Dedekind property if all maximal chains between two elements have the same finite length.

All lattices need not have the Jordan-Dedekind property. For example, in the $N_5$ lattice, shown in Fig. 3, there are two maximal chains from $d$ to $u$. The maximal chain $d \to a \to b \to u$ has three units of length and the other maximal chain $d \to c \to u$ has a length of two units. Thus $N_5$ does not satisfy the Jordan-Dedekind property. It turns out that modularity is closely related to this property.

Theorem 2: [11, pg.41, Th.16] Let $(L, \vee, \wedge)$ be a lattice of finite length with the height function $h$, then the following conditions are equivalent:

1) $L$ is a modular lattice.
2) $L$ has the Jordan-Dedekind property and $h$ is a valuation.

Theorem 3: Let $L$ be a modular lattice of finite length with the height function $h$, then $d_h$ is a metric on $L$.

Clearly $h[x] = 1$ iff $x$ covers $O$. Such elements are called atoms of the lattice. The atoms of the lattice are analogues of the singletons in lattice of sets (one dimensional spaces in the lattice of subspaces).

Definition 11: A geometric modular lattice is a modular lattice of finite height in which every element is a join of atoms. Further, if the geometric modular lattice is distributive, then it will be called geometric distributive.

The lattice of subsets is an example of a geometric distributive lattice and the lattice of subspaces is an example of a geometric modular lattice.

However, all modular (distributive) lattices are not geometric. For example, consider the sublattice (in fact, a chain) $L_1 = \{\phi, \{1\}, \{1, 2\}, \{1, 2, 3\}\}$ of $(\text{Sub}(\mathbb{F}_2), \cup, \cap)$ (shown in part (A) of Fig. 4). $L'$ is not geometric because $\{1, 2, 3\}$ cannot be obtained as a join of atoms of $L_1$ (since there is only one atom in $L'$). $L'$ is distributive since it is a sublattice of distributive lattice $\text{Sub}(\mathbb{F}_2)$, $\cup, \cap$). Therefore $L_1$ is an example of a non-geometric modular lattice.

In order to construct a non-geometric non-distributive modular lattice, we will consider a sublattice of $(\text{Sub}(\mathbb{F}_2), +, \cap)$.

For the sake of presentation, we will represent a vector $(a, b, c)$ by the natural number $a + 2b + 4c$. For example, $(1, 0, 1)$ will be represented as 5. Consider the sublattice $L_2 = \{(\{0\}), (\{1\}), (\{2\}), (\{3\}), (\{1, 2\}), (\{1, 3\}), (\{3, 5\}), \mathbb{F}_3^2\}$ of $(\text{Sub}(\mathbb{F}_2), +, \cap)$. $L_2$ is modular since it is a sublattice of a modular lattice viz. $(\text{Sub}(\mathbb{F}_2), +, \cap)$. $L_2$ is not distributive because it contains a copy of $M_3$ as a sublattice ($M_3$ is non-distributive). It can be verified that $\langle\{3, 5\}\rangle$ cannot be obtained as a join of atoms of $L_2$. Therefore $L_2$ is an example of non-geometric non-distributive modular lattice. Henceforth all the lattices are assumed to be geometric modular unless otherwise mentioned.
III. Lattice Schemes

In order to develop a lattice based framework for Singleton bounds, we need a definition of a code in this framework. In this section, we define ‘Lattice Schemes’ which will serve as analogues of codes. We will show that Hamming space, rank metric space and the projective spaces are examples of lattice schemes. Although some of these observations have been mentioned in [1], we repeat it for the sake of continuity.

A lattice scheme, which is analogous to a code, is defined as follows:

Definition 12: Let \( L \) be a lattice and \( d_h \) be the metric induced by the height function \( h \) of the lattice \( L \). A lattice scheme \( C \) in \( (L,d_h) \) is a subset of \( L \) and the minimum distance of \( C \), denoted by \( d \) is defined as
\[
  d := \min_{a,b \in C, a \neq b} d_h(a,b).
\]

The dimension of a lattice scheme is defined as \( n := h(I) \).

A coding space \( (X,d_X) \) is a metric space where \( X \) is a set and \( d_X \) is a metric on \( X \). A code \( C \) in a coding space \( (X,d_X) \) is a subset of \( X \). The connection between lattice schemes and codes is made precise in the following definition.

Definition 13: Let \( C \) be a lattice scheme in \( (L,d_h) \) and \( \tilde{C} \) be a code in a coding space \( (X,d_X) \). We say that the code \( C \) is equivalent to a lattice scheme \( C \), if there exists a function \( T : X \to L \) that satisfies the following conditions:

1) \( T(\tilde{C}) = C \)
2) \( d_h(T(a), T(b)) = d_X(a,b) \) for all \( a,b \in \tilde{C} \)

\( T \) is called a transform for the code \( \tilde{C} \).

Remark 1: A transform \( T \) of a code is one-one. To prove this fact, assume \( T(a) = T(b) \), then \( d_h(T(a), T(b)) = 0 \). By 2) of Definition 13 this would imply \( d_X(a,b) = 0 \). And since \( d_X \) is a metric, we have \( a = b \).

When a lattice scheme is equivalent to a code, we also say the code is equivalent to the scheme. A transform for a code preserves the distance between any pair of codewords. Therefore whenever a lattice scheme is equivalent to a code, the lattice scheme will have the same minimum distance as the code. The following proposition follows from Definition 13.

Proposition 1: Let \( C \) be a lattice scheme with minimum distance \( d \) that is equivalent to code \( \tilde{C} \) with minimum distance \( \tilde{d} \), then

1) \( d = \tilde{d} \)
2) if \( \tilde{A} \subseteq \tilde{C} \), then there exists \( A \subseteq C \) such that the lattice scheme \( A \) is equivalent to the code \( \tilde{A} \).

Proof: Since \( \tilde{C} \) is equivalent to \( C \), the first part follows from the definition. For the second part, since \( C \) is equivalent to \( \tilde{C} \), there exists a transform \( T \). We define \( A := T(\tilde{A}) \). Clearly \( A \subseteq C \) and the function \( T \) still serves as a lattice transform for the code \( \tilde{A} \). Thus \( A \) is equivalent to \( \tilde{A} \).

Due to the above proposition, given a lattice scheme equivalent to a code, we can talk of the minimum distance without specifying whether it is the minimum distance of the code or the minimum distance of the scheme. From the second part of the Proposition 1 we can infer that the subsets of codes are equivalent to certain subsets of schemes. Therefore, if we prove that a coding space itself is equivalent to some lattice, then any code in the coding space is equivalent to a scheme in the lattice. We use this observation to establish that every binary code is equivalent to a scheme in the power set lattice.

Example 3: Let \( X = n \cdot L = (\text{Pow}(X),\cup,\cap) \) and \( h(A) = |A| \). \( L \) is a geometric distributive lattice and \( d_h(A,B) = |A \cup B| - |A \cap B| = |A \Delta B| \) as seen in the previous section. Consider codes in the coding space \( (\mathbb{F}_2^n, d_H) \) where \( d_H \) is the Hamming distance between two vectors.

We claim that the entire coding space \( \mathbb{F}_2^n \) is equivalent to the power set lattice \( L \). To see this let,
\[
  \phi : \mathbb{F}_2^n \to \text{Pow}(X)
\]
\[
  x \mapsto \text{support}(x).
\]

It can be verified that \( \phi(x + y) = \phi(x) \Delta \phi(y) \) (where \( \Delta \) represents the symmetric difference operator) and that \( \phi \) is onto. Further, \( d_h(\phi(a), \phi(b)) = |\phi(a) \Delta \phi(b)| = |\phi(a+b)| \). The number of elements in \( \phi(a+b) = \text{support}(a+b) \) will be the Hamming weight of \( a+b \). Thus \( |\phi(a+b)| = d_H(a+b,0) = d_H(a,b) \). Therefore, \( \phi \) is the power set lattice transform for the binary code.

Since the map is onto, \( \phi \) is a bijective map. By application of the second part of Proposition 1 we see that every binary code is equivalent to a power set lattice scheme.

The lattice of subspaces, discussed in the previous section, also provide examples of lattice schemes. In a projective lattice, the metric induced by the height function is the subspace distance. Therefore, any subspace code is equivalent to a lattice scheme in the projective lattice.

Example 4: Let \( V \) be a vector space over \( \mathbb{F}_q, L = (\text{Sub}(V),+,\cap) \) is a projective lattice with height function \( h(A) = \text{dim}(A) \). The coding space is \( (\text{Sub}(V),d_S) \) where \( d_S \) represents the subspace distance defined in [2]. For any two subspaces \( A \) and \( B \), \( d_S(A,B) := \text{dim}(A+B) - \text{dim}(A \cap B) \). Since \( d_h(A,B) = h(A \vee B) - h(A \wedge B) = \text{dim}(A+B) - \text{dim}(A \cap B) \), the metric induced by the height function is the subspace distance. The identity map can be a transform in this case. And thus, subspace schemes are equivalent to subspace codes.

Lattice schemes in the above lattice correspond to subspace codes in projective spaces [2], [6]. Certain constant dimension subspace code constructions, described in [12], make use of the rank distance Gabidulin codes [13]. The rank metric codes are actually equivalent to Gabidulin codes since they are ‘lifted’ from Gabidulin codes. We show that rank distance codes are equivalent to certain schemes in the projective lattice. We also show that the ‘lifting’ function is a transform.

Example 5: Let \( (M_{m \times n}^q, d_R) \) denote the space of \( m \times n \) matrices over \( \mathbb{F}_q \). For \( A,B \in M_{m \times n}^q \), define \( d_R(A,B) := \text{rank}(A-B) \). This coding space is the rank distance space. We claim that the rank distance space is equivalent to a scheme in the projective lattice. Consider the projective lattice \( L = (\text{Sub}(\mathbb{F}_q^{m+n}),+,\cap) \) with the height function \( h(A) = \text{dim}(A) \).
Define a transform $T$ as follows:

$$T : M_q^{m \times n} \rightarrow \text{Sub}(\mathbb{F}_q^{m+n})$$

$$A \rightarrow \text{Rowspan}[I \mid A]$$

Notice that $\dim(T(A)) = m$ for any $A$ in $M_q^{m \times n}$. Therefore subspaces whose dimension is not $m$ are not in the range of $T$. Therefore $T$ is an example of a transform that is not onto. The function $T$ defined above is called the ‘lifting of $A$’ in [12]. The authors of [12] establish that $2d_R(A, B) = d_h(T(A), T(B))$. Thus rank metric codes are equivalent to schemes in the projective lattice and $T$ is the projective lattice transform for the rank metric code.

**IV. OUR MAIN RESULT**

All our main results on the bounds and their behavior are derived in this section. We introduce the notion of puncturing a scheme and investigate the effects of puncturing on the minimum distance of a lattice scheme. It will be proved that, after puncturing a scheme, the maximum drop in minimum distance will be two. However, if the lattice is known to be distributive, it is shown that the maximum drop in minimum distance is one. This observation will be applied repeatedly until the minimum distance drops to zero.

We will need the following definition of Whitney number of the second kind, from [14], to state the lattice Singleton bound:

**Definition 14:** The Whitney numbers $c_L(n, k)$ of a lattice $L$ in a lattice with height $h$ and $n = h(I)$ is defined as

$$c_L(n, k) = |\{a \in L | h(a) = k\}|.$$

The Whitney numbers of a lattice count the total number of elements in the lattice of a given height.

**Definition 15:** A scheme $C$ is said to be punctured to $C'$ if $C' = \{ w \land a | a \in C \}$ for some $w \in L$. If $w$ has a height of $h(I) - 1$, the scheme $C$ is said to be punctured by a dimension.

**Remark 2:** Note that for $a \in L$, $\land w := \{ l \land w | l \in L \}$ is a sublattice of $L$ [11]. For two lattice elements $w$ and $w'$ of equal height, we have $c_L(w, k) = c_L(w', k)$. This means that the Whitney numbers of two different punctured lattices remain the same, as long as the elements that puncture the scheme are of the same height.

We need the following lemma (called the ‘distance drop lemma’) to establish the proof of the main theorem later.

**Lemma 1 (Distance drop lemma):** Let $C$ be a scheme in $(L, d_h)$ with minimum distance $d$, and let $C$ be punctured by a dimension to $C'$, then

1) $L$ is distributive $\implies d_{\text{min}}(C') \geq d - 1$

2) In general, $d_{\text{min}}(C') \geq d - 2$.

**Proof:** Proof of 1): We assume $L$ is distributive. Let $\tilde{a} := a \land w$, $\tilde{b} := b \land w$ and $\tilde{a} \lor \tilde{b} := (a \lor b) \land w$. We have to show that

$$d_h(\tilde{a}, \tilde{b}) \geq d - 1$$

for all $a, b \in C$. By the definition of $d_h$,

$$d_h(\tilde{a}, \tilde{b}) = h[\tilde{a} \lor \tilde{b}] - h[\tilde{a} \land \tilde{b}] = h[a \lor b] - h[a \land b] - h[a \land b \land w].$$

Since the lattice is distributive, we can write it as,

$$d_h(\tilde{a}, \tilde{b}) \geq h[a \lor b] - h[a \land b] = h[a \lor b] - h[a \land b] - h[a \land b \land w].$$

The height function is a valuation and thus satisfies $h[x \lor y] + h[x \land y] = h[x] + h[y]$. We use this in the above equation to obtain,

$$d_h(\tilde{a}, \tilde{b}) = h[a \lor b] + h[w] - h[a \lor b \lor w] - h[a \land b \land w].$$

Since $a \lor b \lor w \leq I$, it must be that $h[a \lor b \lor w] \leq h[I] = n$. Using this inequality and $h[w] = n - 1$, we get

$$d_h(\tilde{a}, \tilde{b}) \geq h[a \lor b] + (n - 1) - n - h[a \land b \land w].$$

Clearly $a \land b \land w \leq a \land b$ and therefore $h[a \land b \land w] \leq h[a \land b]$. Using this, the definition of $d_h(\tilde{a}, \tilde{b})$ and the fact that $d$ is the minimum distance of the scheme $C$, we finally get

$$d_h(\tilde{a}, \tilde{b}) \geq d_h(a, b) - 1 \geq d - 1.$$

**Proof of 2):** We have to show that $d_h(a \land w, b \land w) \geq d - 2$ for all $a, b \in C$. Again by the definition of $d_h$,

$$d_h(\tilde{a}, \tilde{b}) = h[a \lor b] - h[a \land b].$$

Repeatedly using the fact that the height function is a valuation and thus satisfies $h[x \lor y] + h[x \land y] = h[x] + h[y]$, we get,

$$d_h(\tilde{a}, \tilde{b}) = h[a] + h[b] + 2h[w] - h[a \land b \land w].$$

Clearly $a \land b \land w \leq a \land b$ and therefore $h[a \land b \land w] \leq h[a \land b]$. Additionally $\tilde{a} \leq I$ and $\tilde{b} \leq I$, which means $h[a], h[b] \leq h[I] = n$. Using this inequality and $h[w] = n - 1$, we get the following:

$$d_h(\tilde{a}, \tilde{b}) \geq h[a] + h[b] + 2(n - 1) - 2n - 2h[a \land b].$$

Using the definition of $d_h(a, b)$ and the fact that $d$ is the minimum distance of the scheme $C$, we finally get,

$$d_h(\tilde{a}, \tilde{b}) \geq d_h(a, b) - 2 \geq d - 2.$$

The distance drop lemma states that in a non-distributive lattice, the drop in the minimum distance after puncturing a dimension, can be at most two units. So it would be interesting to know if it is possible that the drop of two units is exhibited by some scheme in a non-distributive lattice. The following example constructs such a scheme.

**Example 6:** Let $V$ be a three dimensional space, over $\mathbb{F}_2$, spanned by $\{e_1, e_2, e_3\}$. Let $A_1 = \langle e_1, e_2 \rangle$, $A_2 = \langle e_2, e_3 + e_1 \rangle$ and $W = \langle e_2, e_3 \rangle$. We have $d_S(A_1, A_2) = 2$ but $d_S(W \cap A_1, W \cap A_2) = 0$. Note that $A_2 \cap (A_1 + W)$ is $A_2 \cap A_1 + A_2 \cap W$ (that is, the sublattice generated by $A_1, A_2$ and $W$ is not distributive) as expected. If our scheme contained $A_1, A_2$ and $W$, then puncturing the scheme with $W$ would have left $W$ as it is and punctured only the remaining two subspaces.

The above example clearly illustrates that the lack of distributivity in a lattice can drop the distance of a punctured
scheme by two units. We will now derive a Singleton bound for lattice schemes, that establishes an upper bound on the cardinality of the scheme, for a given minimum distance for geometric modular lattices.

**Theorem 4 (Lattice Singleton Bound(LSB))**: If \( (L, d_h) \) is a geometric modular lattice with height \( h \) and \( h(I) = n, d_h \) is the metric induced by the height function, and \( C \) is a scheme of \( L \) with minimum distance \( d \), then

\[
|C| \leq \sum_{k=0}^{n-\alpha_L} c(n - \alpha_L, k)
\]

where

1) \( \alpha_L = d - 1 \), when \( L \) is distributive,
2) \( \alpha_L = \lfloor d - \frac{1}{2} \rfloor \), when \( L \) is modular.

**Proof**: Given the lattice \( L \), pick an element \( w \) of height \( n - 1 \) (which always exists in a geometric modular lattice). Now puncture the lattice by a dimension to get a new geometric modular lattice \( L' \) with height \( n - 1 \) and suppose that drop in minimum distance of the scheme, after puncturing a dimension, is at most \( \beta \). If \( d' \) is the minimum distance of the punctured scheme \( C' \), then \( d' \geq d - \beta \). If \( d - \beta > 0 \), then all elements in the punctured scheme \( C' \) are still distinct. We repeat the puncturing operating on the new lattice. The puncturing is repeated maximum number of times so that the minimum distance of the punctured scheme does not drop to zero. In other words, we keep puncturing the lattice, until the minimum distance of the punctured scheme is just short of zero. Let us say that the original lattice was punctured \( \alpha_L \) times. Since the minimum distance of the punctured scheme is still non zero, the punctured scheme contains exactly the same number of elements as \( C \). At this stage, the minimum distance of the scheme is non-zero and all the elements of the punctured scheme are in a lattice of height \( n - \alpha_L \). Clearly the number of elements in the scheme \( C \) is upper bounded by the total number of elements in the punctured lattice. Thus

\[
|C| \leq \sum_{k=0}^{n-\alpha_L} c(n - \alpha_L, k).
\]

If the minimum distance of the scheme, after being punctured \( \alpha_L \) times, is \( D \), then \( D \geq d - \beta \alpha_L \) and \( D \) is the smallest number such that \( D > 0 \). This implies that \( \beta \alpha_L < d \). From the Lemma 1, we know that \( \beta = 1 \) for a distributive lattice and \( \beta = 2 \) for a modular lattice. Thus \( \alpha_L = d - 1 \) for a distributive lattice and for a modular lattice, \( \alpha_L = \lfloor d - \frac{1}{2} \rfloor \). This completes the proof.

We remark that the bound does not equal \( 2 \), for the case \( d = n \), which should yield only two elements. The bound is weaker for larger minimum distance because we have no information about the range of heights of the elements of the scheme. We can tighten the bound by systematically puncturing and projecting a dimension as done in [2]. Also, as noted in Example 7, puncturing a dimension of a scheme does not reduce the heights of the elements of the scheme in a uniform manner. So we need the following definition.

**Definition 16**: Given two elements \( c \) and \( w \) in a lattice \( L \), define \( \bar{c} \wedge \bar{w} \) to be equal to an element of height \( h(c) - 1 \) that is contained in \( c \wedge w \). In particular, if \( w \) is fixed and \( h(w) = h(I) - 1 \), the set \( \bar{C} \wedge \bar{w} = \{ \bar{c} \wedge \bar{w} | c \in C \} \) is said to be punctured and projected by a dimension.

Thus when \( c \leq w \), \( \bar{c} \wedge \bar{w} \) is arbitrarily chosen to be an element immediately below \( c \) in the Hasse diagram of the lattice. For all other cases, \( \bar{c} \wedge \bar{w} = c \wedge w \). The following example illustrates that puncturing a dimension reduces the heights of different elements of a scheme by different amounts. It also demonstrates that puncturing and projecting by a dimension equally reduces the heights of all elements of a scheme.

**Example 7**: Let \( V \) be a three dimensional space, over \( \mathbb{F}_2 \), spanned by \( \{e_1, e_2, e_3\} \). Let \( A_1 = \langle \{e_1, e_3\} \rangle \), \( A_2 = \langle \{e_2, e_3\} \rangle \) and \( W = \langle \{e_1, e_3\} \rangle \). Fig. 5 shows how puncturing and projecting drops the heights of all elements by one unit. Thus the dimension of \( A_1 \) remains the same after puncturing by \( W \) but the dimension of \( A_2 \) drops by one unit. However, after puncturing and projecting the lattice by \( W \), both \( A_1 \) and \( A_2 \) drop by a height of one unit. To be precise, define \( E_3 := W \wedge A_2 = \langle \{e_3\} \rangle \) and observe that \( W \wedge A_2 = W \wedge A_2 = E_3 \). But \( W \wedge A_1 = W \). To define \( W \wedge A_1 \) we need to choose a one dimensional subspace of \( A_1 \). For instance, we can choose \( W \wedge A_1 = E_3 \).

We can now establish that puncturing and projecting a dimension of a scheme can drop the minimum distance of the scheme by at most two units. This lemma is useful since it tells us that every time we puncture and project by a dimension, all the elements in the scheme drop once in height.

**Lemma 2**: Let \( C \) be a scheme in a lattice \( (L, d_h) \) with minimum distance \( d \), and let \( h(I) = n \) and let \( w \in L \) such that \( h(w) = n - 1 \). If the maximum height of \( C \) was \( M \) and the minimum height of \( C \) was \( m \), then the maximum height of \( \bar{C} \wedge \bar{w} \) is \( M - 1 \) and the minimum height is \( m - 1 \). Additionally \( d_{\min}(C \wedge w) \geq d - 2 \).
Applying the LSB theorem, we get, as a corollary to the LSB theorem.

By the definition of $d_h$,

$$d_h(a \wedge w, b \wedge w) = h[a \wedge w] + h[b \wedge w] - 2h[a \wedge w \wedge b \wedge w].$$

From the definition of $x \wedge w$, it follows that $x \wedge w \leq x \wedge w$ and thus $h[x \wedge w] \leq h(a \wedge w)$ for all $x \in L$ and thus,

$$d_h(a \wedge w, b \wedge w) \geq (h[a] - 1) + (h[b] - 1) - 2h[a \wedge b]$$

and therefore from the formula for height we get,

$$d_h(a \wedge w, b \wedge w) \geq d_h(a, b) - 2 \geq d - 2.$$

We will need Lemma 2 to get the following improvement on the code size.

**Theorem 5:** Let $C$ be a scheme in a geometric modular lattice $L$ with minimum distance $d$. Let $m$ denote the smallest height of all the elements in $C$ and $M$ denote the largest height of all the elements in $C$. Then,

$$|C| \leq \sum_{k=m-\alpha_L}^{M-\alpha_L} c_L(n - \alpha_L, k).$$

**Proof:** Let $w$ be an element of height $n - 1$ and $L' = L \wedge w$. By Lemma 2, the punctured and projected scheme in $L'$ has a maximum height of $M - 1$, a minimum height of $m - 1$ and a minimum distance drop of at most two units. Now the proof proceeds in a manner similar to the proof of the Theorem 4. After puncturing $\alpha_L$ times, the elements of the scheme will have a maximum height of $M - \alpha_L$ and a minimum height of $m - \alpha_L$ and the theorem is proved.

We will now apply Theorem 4 and Theorem 5 to two important lattice schemes (namely the power set lattice and the projective lattice) and derive the corresponding LSB. The LSB that we obtain coincides with the Singleton bound found in the literature. First, we derive the classical Singleton Bound as a corollary to the LSB theorem.

**Corollary 1:** Let $C$ be a code in $(\mathbb{F}_2^n, d_H)$, with minimum distance $d$, then $|C| \leq 2^{n-d+1}$.

**Proof:** In Example 3, $c_L(n - \alpha_L, k)$ is the number of subsets of size $k$ in the scheme $C$, given that $v(I) = n - \alpha_L$. Using the fact that $L$ is geometric and distributive, $\alpha_L = d - 1$. First we observe that,

$$c_L(n - d + 1, k) \leq |\{A \in L | A| = k\}|$$

and

$$|\{A \in L | A| = k\}| = \binom{n-d+1}{k}.$$

Applying the LSB theorem, we get,

$$|C| \leq \sum_{k=0}^{n-d+1} \binom{n-d+1}{k} = 2^{n-d+1}$$

which is the Singleton bound for $(\mathbb{F}_2^n, d_H)$.

Now we derive the KKS bound reported in [2]. It follows as a direct corollary to Theorem 5 when the lattice is chosen to be the lattice of subspaces.

**Corollary 2 (KKS Bound):** If $m = M = l$ and $\alpha_L = \lceil \frac{d-1}{2} \rceil$, then

$$|C| \leq \frac{n - \alpha_L}{l - \alpha_L} q^l.$$

**Proof:** Let $L = (\text{Sub}(V), +, \cap)$ where $C$ is chosen to be a subset of the Grassmanian $G(n, l)$. Then $m = M = l$ and the lattice coefficients $c_L(n, l) = \lceil \frac{n}{l} \rceil q^l$. Now apply Theorem 5 to $C$.

The distance drop lemma, used in the main theorem, along with Example 6 clearly shows that at every step of puncturing the distance can drop by at most two units. On the other hand, one can construct examples where distance drop is one unit. Now suppose some scheme achieves the LSB (and thus the KKS bound). Then that scheme has elements which consistently drop by a distance of two units irrespective of which element is puncturing it. And this should happen at every puncturing step until the minimum distance drops to zero. Since this seems highly unlikely, we conjecture the following:

**Conjecture:** There are no schemes that can achieve the LSB for projective spaces. In particular, there are no constant dimension codes that can achieve the KKS bound.

**V. A NEW UPPER BOUND FOR PROJECTIVE SPACE CODES**

It is clear that many examples fit into the framework of lattice schemes and the proposed LSB specializes to the known Singleton bounds in literature. In this section, we will show that the LSB gives a new upper bound when applied to projective spaces. A family of non-constant dimension code constructions in projective spaces have been reported by [7] and [10]. Our LSB plots show that the code sizes, of both reported codes, are near optimal for certain fixed values of the coding parameters.

Singleton bound in projective spaces will be specified using Gaussian numbers (they are the $q$-analogues of binomials [15]). Lower bounds on code sizes based on sphere covering methods can be found in [6]. Upper bounds on code sizes for projective space codes, found in the literature, are for constant dimension codes. The following bound is an upper bound on the code size of a non-constant dimension code in a projective space.

**Corollary 3 (Singleton Bound for projective spaces):** Let $C$ be a code in $(\text{Sub}(V), d_S)$ (where $V$ is vector space over $\mathbb{F}_q$), with minimum distance $d$, then

$$|C| \leq \sum_{k=0}^{n-d+1} \left[ \binom{n-d+1}{k} q^k \right].$$

where $\binom{n}{k}_q$ denotes the Gaussian number.

**Proof:** The $L = (\text{Sub}(V), d_v)$ lattice with $v(A) = \dim(A)$ is a modular geometric lattice. We note that

$$c_L(n - \alpha_L, k) \leq |\{A \in L | \dim A = k\}|.$$
Bounds for $q = 2$ and $d = 4$

Fig. 6. A plot that compares code sizes of different non-constant dimension codes and a lower bound on the code size. Note that the KhKs code sizes are within three bits from our upper bound. The subspaces are assumed to be over $F_2$ and the minimum distance is fixed at 4.

The Gaussian number $\begin{bmatrix} N \\ K \end{bmatrix}_q$ is the total number of $K$-dimensional subspaces of an $N$-dimensional space over $F_q$ and thus by Theorem 4,

$$|C| \leq \sum_{k=0}^{k=n-\alpha_L} \begin{bmatrix} n-\alpha_L \\ k \end{bmatrix}_q$$

where $\alpha_L = \lfloor \frac{d-1}{2} \rfloor$.

The bound is weak when the minimum distance $d$ is comparable to the code dimension $n$. However when the minimum distance is smaller than code dimension, the tightness of the bound is not apparent. Therefore we investigate the behaviour of our bounds, at such ranges, by plotting it with other bounds in the literature. We will compare our bound (LSB) to the Gilbert Varshamov bound (EV-GVB) proposed in [6] for various values of the minimum distance. Further, we will plot points achieved by various codes in the literature.

The plot is shown in Fig. 6. The minimum distance of the projective code and the finite field size has been fixed at 4 and 2 respectively, throughout this section. The plot clearly shows our upper bound above the EV-GV lower bound. The points marked ‘EtzSilb codes’ and ‘KhKs code’ are the code parameters reported in [7] and [10] respectively, for $q = 2$ and $d = 4$.

Fig. 6 shows that the EtzSilb codes and KhKs codes are close to optimal for $q = 2$ and $d = 4$. The KhKs code sizes are roughly 3 bits away from the upper bound. It has already been observed that the distance drop in projective spaces is variable and thus we believe that our bound is weak for larger values of $d$.

VI. DISCUSSION

In this paper, we introduced the notion of lattice schemes which serve as analogues of codes. We derived a general notion of Singleton bound for which the classical Singleton bound for binary codes and the Singleton-like bound for constant dimension subspace codes were special cases. We proved that puncturing a dimension gives a tight bound for distributive lattices but not for projective lattices. However, it was seen that puncturing and projecting a dimension gives a tighter bound, for projective lattices. This leads us to conjecture that it is not possible to achieve the KKS bound.

The upper bound derived in the paper seems to be tighter when the minimum distance is much smaller than the code dimension. A next step would be to tighten the bounds for large minimum distances. It would be interesting to investigate whether there exists lattice schemes that achieve the LSB with equality. In particular, it would be very interesting to know if there exists a Reed Solomon-like scheme which specializes to the different counterparts in binary and subspace codes. Also, whether quantum codes are lattice schemes can be investigated.

REFERENCES

[1] M. Braun, “On lattices, binary codes, and network codes,” Advances in Mathematics of Communications, vol. 5, pp. 225 –232, September 2011.
[2] R. Koetter and F. Kschischang, “Coding for errors and erasures in random network coding,” IEEE Transactions on Information Theory, vol. 54, pp. 3579 –3591, Aug. 2008.
[3] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal, “Cyclic orbit codes,” http://arxiv.org/abs/1112.7238, 2011.

[4] 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.

[5] P. Delsarte and V. Levenshtein, “Association schemes and coding theory,” IEEE Transactions on Information Theory, vol. 44, pp. 2477 –2504, Oct 1998.

[6] T. Etzion and A. Vardy, “Error-correcting codes in projective space,” IEEE Transactions on Information Theory, vol. 57, pp. 1165 –1173, Feb. 2011.

[7] T. Etzion and N. Silberstein, “Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams,” IEEE Transactions on Information Theory, vol. 55, pp. 2909 –2919, July 2009.

[8] N. Silberstein and T. Etzion, “Representation of subspaces and enumerative encoding of the Grassmannian space,” http://arxiv.org/abs/0911.3256, 2009.

[9] N. Silberstein and T. Etzion, “Codes and designs related to lifted MRD codes,” in IEEE International Symposium on Information Theory Proceedings (ISIT), pp. 2288 –2292, 31 2011-Aug. 5 2011.

[10] A. Khaleghi and F. Kschischang, “Projective space codes for the injection metric,” in 11th Canadian Workshop on Information Theory, 2009., pp. 9 –12, May 2009.

[11] G. Birkhoff, Lattice theory. Colloquium Publications, American Mathematical Society, 1995.

[12] 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, September 2008.

[13] E. Gabidulin, “Theory of codes with maximum rank distance,” Problems Information Transmission, vol. 21, no. 1, pp. 1–12, 1985.

[14] R. Stanley, Enumerative Combinatorics, Vol.1. Cambridge University Press, 2002.

[15] J. Lint and R. Wilson, A Course in Combinatorics. Cambridge University Press, 2001.