US 20250259094A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0259094 A1**

JOSHUA et al. (43) **Pub. Date: Aug. 14, 2025**

(54) **QUANTUM ERROR CORRECTING CODES FROM HIGHER GRASSMANN CODES**

(71) Applicants: **Ohio State Innovation Foundation**, Columbus, OH (US); **The Administrators of the Tulane Educational Fund ("TU")**, New Orleans, LA (US); **The Curators of the University of Missouri, through its University Constituent, the University of**, St. Louis, MO (US)

(72) Inventors: **Roy JOSHUA**, Dublin, OH (US); **Mahir Bilen CAN**, New Orleans, LA (US); **Ravindra GIRIVARU**, Clayton, MO (US)

(21) Appl. No.: **18/857,325**

(22) PCT Filed: **Apr. 18, 2023**

(86) PCT No.: **PCT/US2023/018890**

§ 371 (c)(1),
(2) Date: **Oct. 16, 2024**

Related U.S. Application Data

(60) Provisional application No. 63/331,979, filed on Apr. 18, 2022.

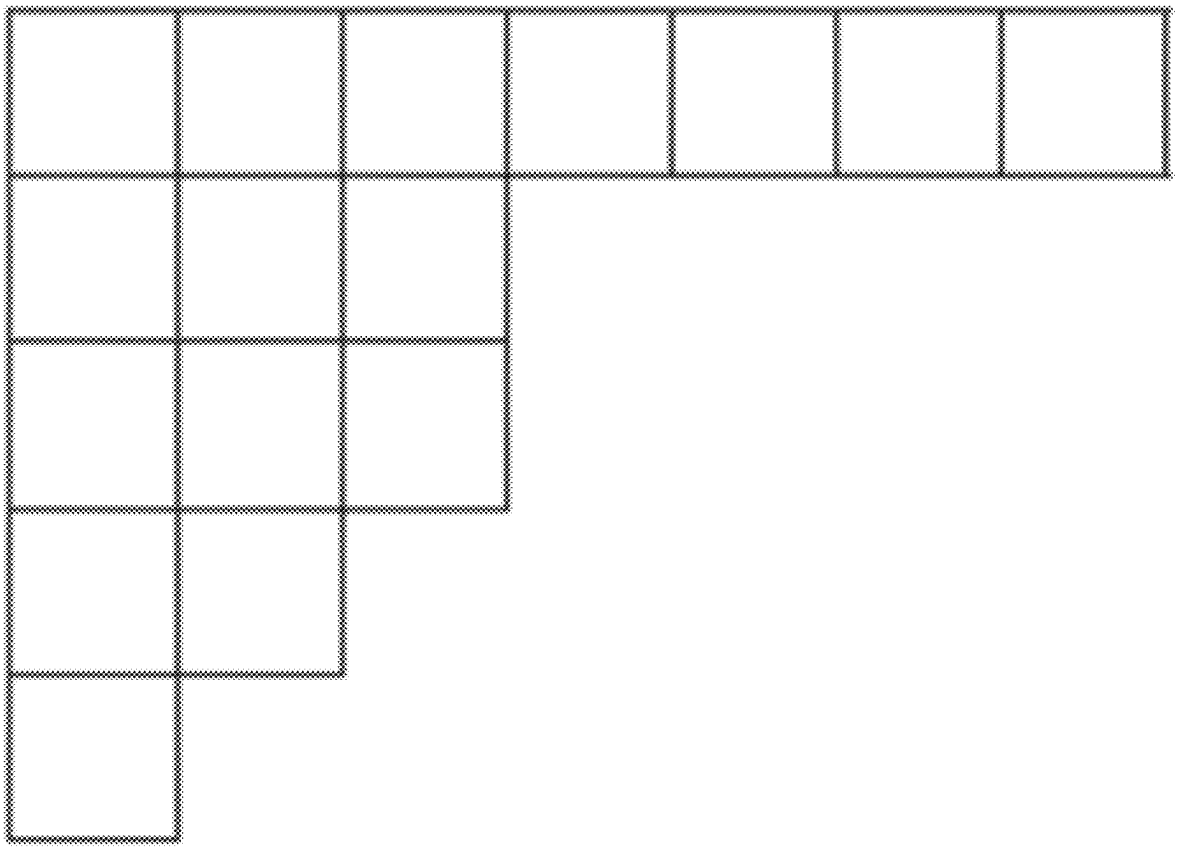
Publication Classification

(51) **Int. Cl.**
G06N 10/70 (2022.01)

(52) **U.S. Cl.**
CPC ***G06N 10/70*** (2022.01)

(57) **ABSTRACT**

Systems and methods to construct Quantum Error Correcting codes from Higher Grassmann Codes. The present disclosure is directed to algebraic codes obtained from families of imbeddings of the Grassmannian, constructed as the composition of a diagonal imbedding followed by a Segre imbedding into various high dimensional projective spaces. As a result, a large family of new error correcting codes is obtained, and the parameters of such codes are determined.



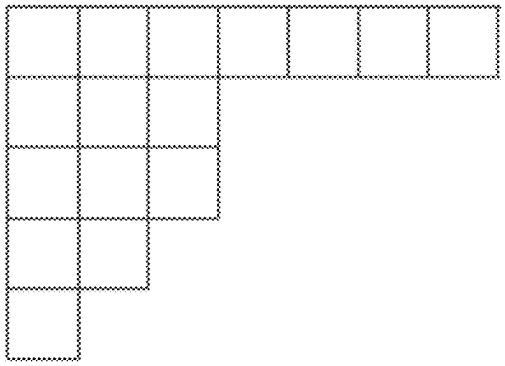


FIG. 1

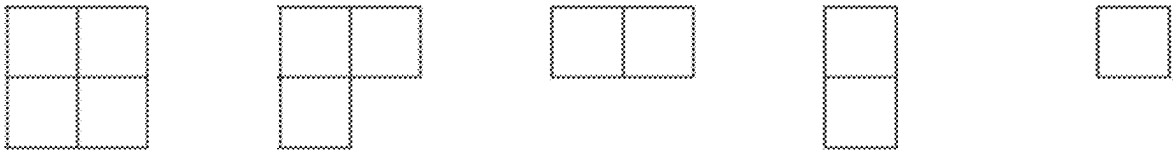


FIG. 2

$$\begin{array}{ccc} & & (\Lambda^l V) \setminus \{0\} \\ & & \downarrow \\ \mathbf{p} : Gr(l, V) & \longrightarrow & \mathbb{P}^{\binom{m}{l}-1} \end{array}$$

FIG. 3

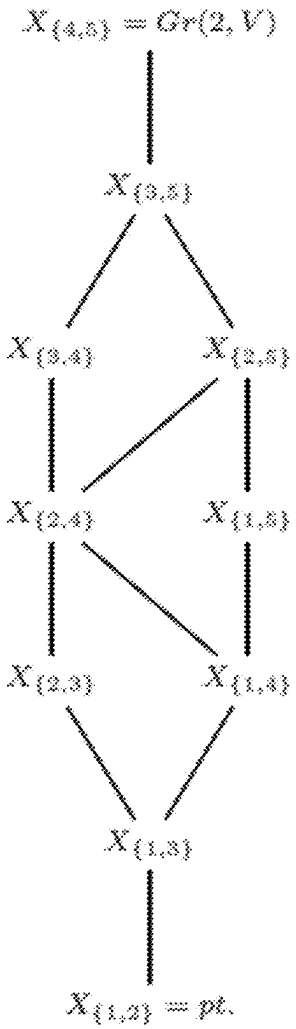


FIG. 4

1	1	2	2	5
2	2	3	4	
3	4	5		

FIG. 5

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)
(2, 1)	(2, 2)	(2, 3)	(2, 4)	
(3, 1)	(3, 2)	(3, 3)		

FIG. 6

0	1	2	3	4
−1	0	1	2	
−2	−1	0		

FIG. 7A

7	6	5	3	1
5	4	3	1	
3	2	1		

FIG. 7B

FIG. 8

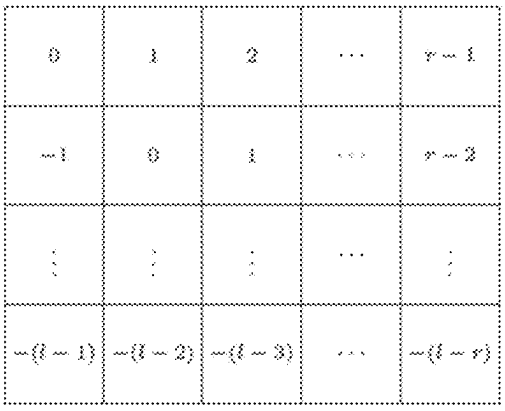


FIG. 9A

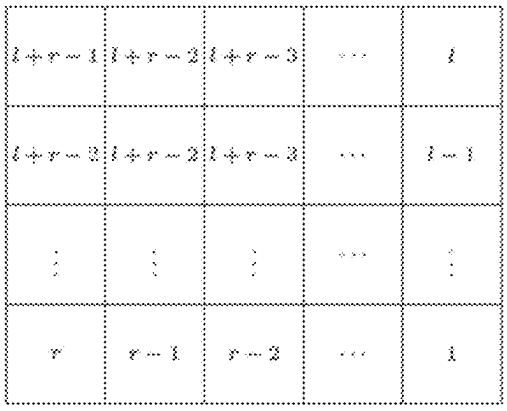


FIG. 9B

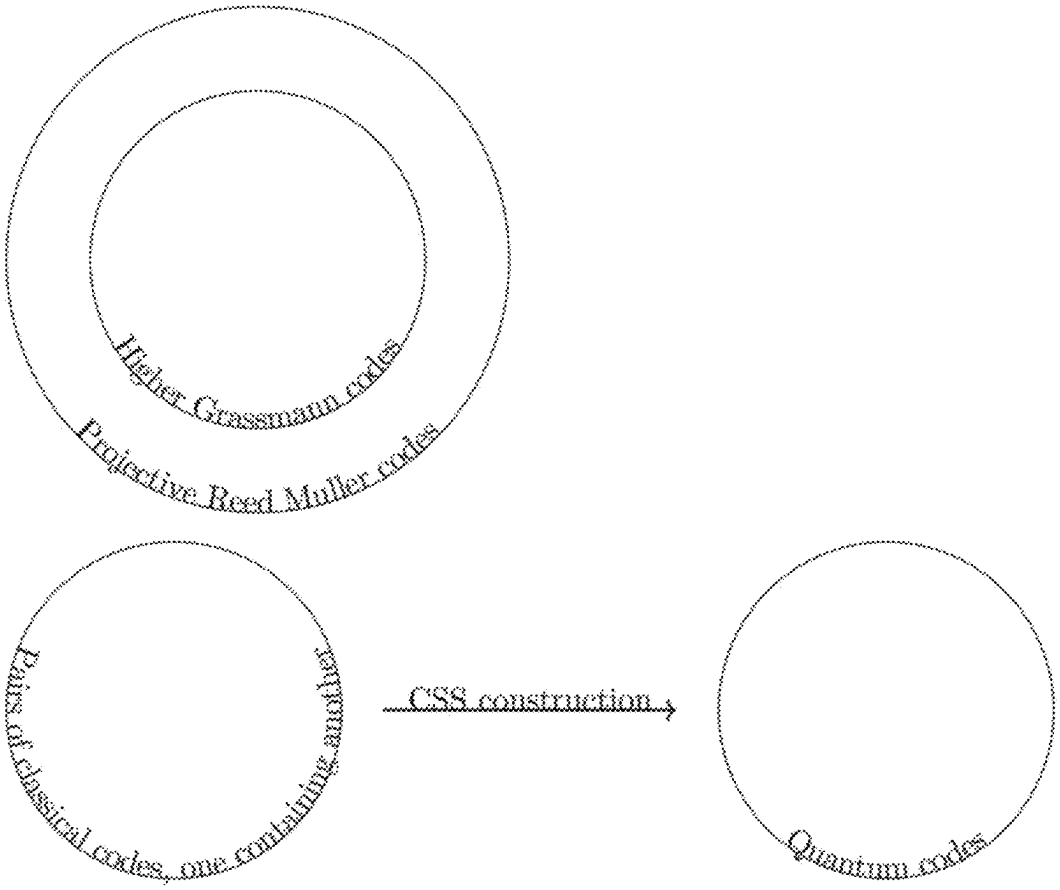

Higher Grassmann codes
Projective Reed Muller codes
Pairs of classical codes, one containing another
CSS construction
Quantum codes

FIG. 10

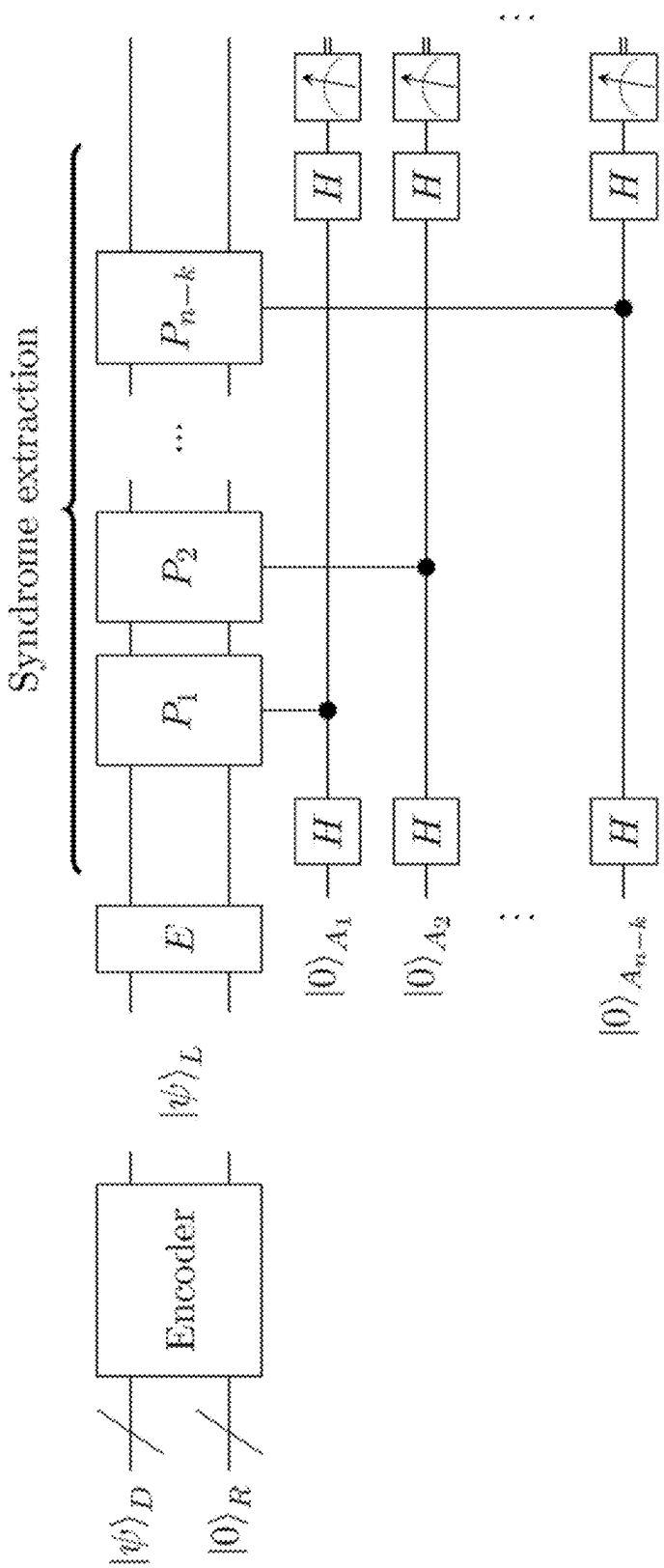

Syndrome extraction
Encoder
E
P_1
P_2
P_{n-k}
H
$|\psi\rangle_D$
$|0\rangle_R$
$|\psi\rangle_L$
$|0\rangle_{A_1}$
$|0\rangle_{A_2}$
$|0\rangle_{A_{n-k}}$

FIG. 11

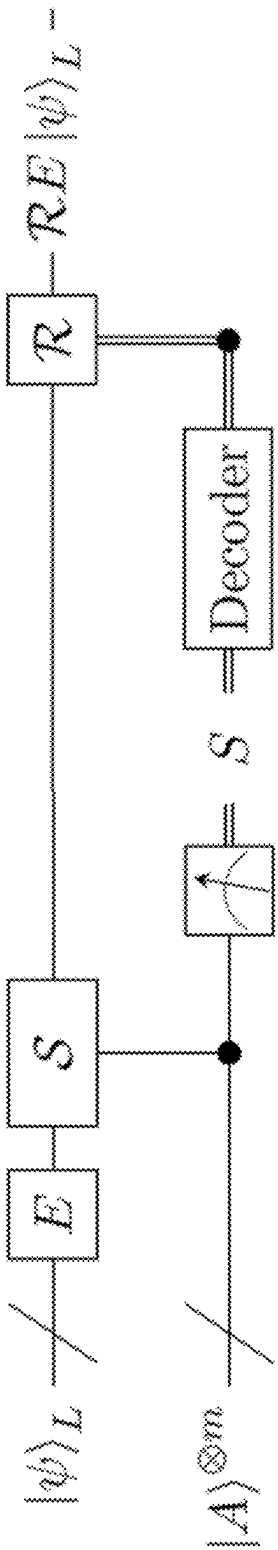


FIG. 12

QUANTUM ERROR CORRECTING CODES FROM HIGHER GRASSMANN CODES

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This is a national phase application under 35 U.S. C. § 371 that claims priority to PCT/US2023/018890, filed Apr. 18, 2023, that further claims priority to U.S. Provisional Patent Application No. 63/331,979, filed Apr. 18, 2022, each entitled "QUANTUM ERROR CORRECTING CODES FROM HIGHER GRASSMANN CODES," the disclosures of which are incorporated herein by reference in their respective entireties.

FIELD OF THE INVENTION

[0002] The present invention relates to error correcting codes, and more specifically, to the construction of Quantum Error Correcting codes from the Higher Grassmann Codes.

BACKGROUND

[0003] Error correcting codes play an important role: classically they have been used to correct transmission errors, but lately these also play a key role in quantum computation in the form of quantum error correcting codes which prevent decoherence. One important class of error correcting codes are the ones constructed using the methods of Algebraic geometry from algebraic varieties defined over finite fields. The Grassmann varieties form a familiar class of well understood algebraic varieties. For example, the Grassmann variety of k-dimensional subspaces of a fixed n-dimensional vector space over a finite field F_q is a smooth projective variety: the way it gets the structure of a projective variety is by making use of the well-known Plucker imbedding. The corresponding Grassmann code is obtained by evaluating the sections of the restriction of the canonical line bundle on the ambient projective space at the F_q-rational points on the Grassmannian. Such Grassmann codes are generalization of Reed-Muller codes, which have been used in classical error correction. To date, the only Grassmann codes considered have been codes obtained from the classical Plucker imbedding, though there are many other possible projective imbeddings.

SUMMARY

[0004] The present disclosure is directed to algebraic codes obtained from families of imbeddings of the Grassmannian, constructed as the composition of a diagonal imbedding followed by a Segre imbedding into various high dimensional projective spaces. As a result, a large family of new error correcting codes is obtained and the parameters of such codes are determined.

[0005] In accordance with the present disclosure, an apparatus to encode and decode quantum [[n; k; d]] stabilizer codes is disclosed. The apparatus includes an encoder that entangles a quantum data register $|\psi\rangle_D=|\psi_1\psi_2\ldots\psi_k\rangle$ with redundancy qubits $|0\rangle_R=|0_1 0_2\ldots 0_{n-k}\rangle$ to create a logical qubit $|\psi\rangle_L$; and stabilizer check logic that, after encoding, performs a sequence of n−k stabilizer checks P_i on the quantum data register and that copies each result to an ancilla qubit A_i. A subsequent measurement of the ancilla qubits provides an m-bit syndrome.

[0006] In accordance with yet another aspect of the disclosure, a method to encode and decode quantum [[n; k; d]] stabilizer codes error correcting codes from higher Grassmann codes is disclosed. The method includes generating higher Grassmann codes that are imbedded as sub-codes of in a higher-order projective space ($\mathbb{P}^m$) that corresponds to line bundles $\mathcal{O}(v)$ on the Grassmann variety; entangling a quantum data register $|\psi\rangle_D=|\psi_1\psi_2\ldots\psi_k\rangle$ with redundancy qubits $|0\rangle_R=|0_1 0_2\ldots 0_{n-k}\rangle$ that use the higher Grassmann codes to create a logical qubit $|\psi\rangle_L$; performing a sequence of n−k stabilizer checks P_i on the quantum data register and copying each result to an ancilla qubit A_i; and performing a subsequent measurement of the ancilla qubits to provide an m-bit syndrome.

[0007] In accordance with yet another aspect, a method for active recovery in a quantum error correction code is disclosed that includes performing an error process E on a logical qubit $|\psi\rangle_L$ of an [[n, k, d]] stabilizer code; measuring a generating set of stabilizers S on a logical state to yield an m-bit syndrome $\mathcal{S}$; and processing the m-bit syndrome $\mathcal{S}$ by a decoder to determine a best recovery operation $\mathcal{R}$ to return the logical state to a codespace. After the recovery operation has been applied, the output of an error correction cycle is $\mathcal{R}E|\psi\rangle_L$.

[0008] The following is a non-exhaustive list of the advantages these codes have over the classical Grassmann codes:

- **[0009]** First the dimension of the new codes we obtain are greater than the dimension of the classical Grassmann codes
- **[0010]** Over large fields, the minimum distance of our codes are asymptotically the same as those of the classical Grassmann codes.
- **[0011]** One key application of these new codes is to quantum error correction, which we plan to explore.

[0012] Thus, a significant advantage is gained by considering these geometric codes.

[0013] The foregoing illustrative summary, as well as other exemplary objectives and/or advantages, and the manner in which the same are accomplished, are further explained within the following detailed description and its accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] A detailed description of certain aspects of the present disclosure in accordance with various example implementations will now be provided with reference to the accompanying drawings. The drawings form a part hereof and show, by way of illustration, specific implementations and examples. In referring to the drawings, like numerals represent like elements throughout the several figures.

[0015] FIG. **1** illustrates the Young diagram of (7,3,3,2,1);

[0016] FIG. **2** illustrates the Young diagrams of the integer partitions whose Young diagram fits in a 2×2 grid;

[0017] FIG. **3** illustrates the Plücker coordinates of Gr(l, V);

[0018] FIG. **4** illustrates the Grassmann variety Gr(2, V) and its Schubert varieties;

[0019] FIG. **5** illustrates a semistandard Young tableau of shape (5,4,3);

[0020] FIG. **6** illustrates the coordinates of the boxes of (5,4,3);

[0021] FIGS. **7**A and **7**B illustrate the content and hook lengths of the boxes of (5,4,3);

[0022] FIG. **8** illustrates the set of SSYT of shape (2,2) with entries from {1,2,3};

[0023] FIGS. **9**A and **9**B illustrate the contents and hook lengths for the boxes of (r, . . . , r, 0, . . . , 0);

[0024] FIG. **10** illustrates a schematic of Grassmann codes as subset of Projective RM codes;

[0025] FIG. **11** illustrates a circuit diagram Circuit illustrating the structure of an [[n; k; d]] stabilizer code; and

[0026] FIG. **12** illustrates a general procedure for active recovery in a quantum error correction code.

DETAILED DESCRIPTION

[0027] Unlike digital computing, error correction plays a key role in quantum computing. This is because of the effect of decoherence, where the data will get corrupted very rapidly by interference with the environment, unless error correction is applied at nearly every stage of the computational process. As such, any improvements in quantum error correcting technology is of immense importance presently.

Introduction

[0028] Throughout the disclosure, $\mathbb{F}_q$ will denote the finite field with q elements, where q is a power of a prime number, p. Moreover, we will restrict to schemes of finite type defined over such a finite field. Let X denote the Grassmann variety of l-dimensional subspaces of a fixed m-dimensional vector space V. One way to obtain the projective variety structure on X is via the Plücker embedding p: $X \hookrightarrow$

$$\mathbb{P}^{\binom{m}{l}-1}$$

The corresponding Grassmann code is obtained by evaluating sections of the line bundle on X obtained as the restriction of the canonical line bundle on

$$\mathbb{P}^{\binom{m}{l}-1}$$

at the $\mathbb{F}_q$-rational points on X. The Grassmann codes are natural generalizations of the well-known Reed-Müller codes. A significant advantage in efficiency is gained by considering these geometric codes. Indeed, already in the case of projective spaces, the performance of the projective Reed-Müller codes, compared to the classical generalized Reed-Müller codes, are much better. The parameters for a general Grassmann code over $\mathbb{F}_q$ was computed.

[0029] In the present context, by a projective embedding of an algebraic variety or a scheme X, we mean a closed immersion of X into a projective space $\mathbb{P}^m$. One may consider many other projective embeddings of the Grassmannian other than the Plücker embedding. For example, let ι: Gr(l, V)$\rightarrow\mathbb{P}((\wedge^l V)^{\otimes r})$ denote the projective embedding of Gr(l, V) that is obtained by composing the diagonal Plücker embedding with the r-fold Segre embedding of $\Pi^r\mathbb{P}(\wedge^l V)$. The resulting code is obtained by evaluating the global sections of the restriction of the canonical line bundle on the corresponding projective space to the Grassmannian, at the $\mathbb{F}_q$-rational points of the Grassmannian. The present disclosure describes a methodology to explicitly determine the parameters of all such codes obtained from the Grassmannian. This is part of a larger effort to compute parameters of codes produced from the large class of algebraic varieties called projective spherical varieties, which contain as special cases the class of all projective embeddings of Grassmannians, flag varieties as well as toric varieties.

[0030] When l=1, the Grassmann variety Gr(l, V) is equal to the projective space of lines in V, that is, $\mathbb{P}(V)\cong\mathbb{P}^{m-1}$. In this case we get the projective Reed-Müller codes; for every $r\in\mathbb{N}$, the relevant embedding is provided by the r-th symmetric power of V. Herein, we consider higher dimensional projective spaces to embed the Grassmann variety, such as via the composition of the diagonal Plücker embedding with the Segre embedding.

[0031] Let x denote a variable and let a be a positive integer. Then the a-th rising factorial of x, denoted by $x^{(a)}$, is the product $x^{(a)}=x(x+1)\ldots(x+a-1)$.

[0032] Let q denote a power of a prime number p. It is convenient to denote by $[m]_q$ the polynomial

$$1+q+\ldots+q^{m-1}=\frac{q^m-1}{q-1},$$

which is often called the q-analog of m since its evaluation at q=1 is m. The q-factorial of m is defined by $[m]_q!:=[m]_q[m-1]_q\ldots[2]_q[1]_q$. As convention, we set $[0]_q:=1$. For $l\in\{0,\ldots,m\}$, the q-binomial coefficient

$$\begin{bmatrix} m \\ l \end{bmatrix}_q$$

is defined by

$$\begin{bmatrix} m \\ l \end{bmatrix}_q := \frac{[m]_q!}{[m-l]_q![l]_q!}.$$

[0033] It is well-known that, if q is a power of a prime number, then

$$\begin{bmatrix} m \\ l \end{bmatrix}_q$$

is the $\mathbb{F}_q$-rational points of the Grassmann variety of l-dimensional subspaces of an m-dimensional vector space. Also, there is an elementary combinatorial interpretation of

$$\begin{bmatrix} m \\ l \end{bmatrix}_q$$

in terms of partitions of integers.

[0034] Moreover, one may recall the following standard terminology used in coding theory. A k-dimensional vector subspace W in an n-dimensional vector space V defined over $\mathbb{F}_q$ is called an $[n, k, d]_q$-code. Here, d is defined as the minimum of the distances between distinct elements of W; the distance is defined by the number of coordinates where two vectors differ from each other. The integer n is often called the length of the code, and k is called the dimension of the code.

[0035] Let $\{e_1, \ldots, e_n\}$ denote the standard basis for $\mathbb{F}_q^n$, and let $x_1, \ldots, x_n$ denote the corresponding coordinate functionals on $\mathbb{F}_q^n$. An $[n, k, d]_q$-code $W \subset \mathbb{F}_q^n$ is said to be nondegenerate if W is not contained in any of the following coordinate hypersurfaces:

$$H_i := \{v \in \mathbb{F}_q^n : x_i(v) = 0\} \cong \mathbb{F}_q^{m-1} (i \in \{1, \ldots, n\}).$$

[0036] There is a 1-1 correspondence between the set of equivalence classes of nondegenerate $[n, l, d]_q$-codes and the set of equivalence classes of projective $[n, k, d]_q$-systems, which are defined as follows.

[0037] Let X be an algebraic variety with n $\mathbb{F}_q$-rational points. Let $\varphi: X \to \mathbb{P}^{m-1}$ be an embedding and let $x_1, \ldots, x_n$ denote the images of the $\mathbb{F}_q$-rational points of X in $\mathbb{P}^{m-1}$. Let E denote the $\mathbb{F}_q$-vector space $\mathbb{F}_q^m$, and let $y_1, \ldots, y_n$ denote (arbitrary) liftings of $x_1, \ldots, x_n$ to $E\backslash\{0\}$ in the given order. Then we get an evaluation map on the linear forms of E,

$$\begin{aligned} ev: E^* &\to \mathbb{F}_q^n \\ f &\mapsto (f(y_1), \ldots, f(y_n)). \end{aligned} \tag{1.1}$$

[0038] The image of ev, denoted by C, is the projective $[n, k, d]_q$-system associated with φ. Note that the length of C is n, its dimension is k=m−dimker(ev), and its minimum distance is given by

$$d = \min\{|X(\mathbb{F}_q)| - |X(\mathbb{F}_q) \cap ker(f)| : f \in E^* \text{ and } X(\mathbb{F}_q) \not\subset ker(f)\}.$$

[0039] As before, let V be an m dimensional vector space over $\mathbb{F}_q$. The points in the image of the Plücker embedding p:

$$Gr(l, V) \to \mathbb{P}^{\binom{m}{l}-1}$$

can be viewed as projective $[n, k, d]_q$-systems, where

$$n = \begin{bmatrix} m \\ l \end{bmatrix}_q \text{ and } k = \binom{m}{l}.$$

These projective systems (or rather the codes corresponding to these projective systems) are called the (classical) Grassmann codes.

[0040] The material in paragraphs [0024] through [0037] and [0041] through [0058] are background material, setting up the framework for the subsequent discussion. One main result is discussed in paragraph [0040] as well as in paragraphs [00109] through [00113] and another main result is discussed in paragraph [00152] The first step in our algorithm is discussed in paragraphs [0060] through [0066], while the second step is discussed in paragraphs [00119] through [00124]. The third step is discussed in paragraphs [00125] through [00150] and the fourth step is discussed in paragraphs [00153] through [00160]. The fifth and final step of our algorithm is discussed in paragraph [00160]. The implementation details of our algorithm are discussed in paragraphs [00161] through [00166].

[0041] Adopting the above notation, we now present a special case of our main theorem, which is recorded as Theorem 4.1 in the sequel.

[0042] Theorem 1.3. Let $\iota: Gr(l, V) \to \mathbb{P}((\wedge^l V)^{\otimes r})$ denote the projective embedding of Gr(l, V) that is obtained by composing the diagonal Plücker embedding with the r-fold Segre embedding of $\Pi^r \mathbb{P}((\wedge^l V)$. If C is the projective $[n, k, d]_q$-system corresponding to ι, then for every sufficiently large prime characteristic p>0, the parameters of C satisfy the following conditions:

1. $n = \begin{bmatrix} m \\ l \end{bmatrix}_q = \dfrac{[m-1]_q \cdots [m-l+1]_q}{[1]_q [2]_q \cdots [l]_q}$
2. $k = \dfrac{m^{(r)}(m-1)^{(r)} \cdots (m-l+1)^{(r)}}{1^{(r)} 2^{(r)} \cdots l^{(r)}}$,
3. $q^{l(m-l)} - rq^{l(m-l)-1} \le d \le q^{l(m-l)} - (r-1)q^{l(m-l)-1}$.

[0043] We know that the upper bound for the minimum distance is achieved for r=1 as well as for l=1. We conjecture that the upper bound is always achieved. Note that as a polynomial in q, the leading term of n in Theorem 1.3 is $q^{l(m-l)}$. Also, the coefficient of $q^{l(m-l)-1}$ in n is **1**. (We will justify these statements in Section **2** by using a simple, well-known combinatorial argument.) Then the leading term of the difference n−d is given by $rq^{l(m-l)-1}$. It follows that, if we fix r, then for every sufficiently big q, the difference n−d is greater than k. In other words, our codes satisfy the Singleton bound for sufficiently large values of q. Let us point out that there is an effective way, due to Jantzen, to check how small the characteristic p can be in order for our theorem to hold.

[0044] Next, we want to point out some facts about the parameters of our codes. First of all, for r>1, it is easy to see by an inductive argument that the dimensions of our codes are all greater than

$$\binom{m}{l},$$

which is the dimension of Grassmann codes obtained from the Plücker embedding. On the other hand, it is already apparent from the r=2 case of Theorem 1.3 that our codes may have smaller minimum distance compared to the ordinary Grassmann codes (r=1). Nevertheless, as $q \to \infty$, the dominating term of the minimum distance of our code is also given by $q^{l(m-l)}$. Therefore, on finite fields with big characteristic exponents, our codes become more advantageous compared to the ordinary Grassmann codes.

[0045] The present disclosure is structured as follows. Below, we set up our notation, and we review some basic representation theory and algebraic geometry facts regarding Grassmann and Schubert varieties. In Section 3, we analyze the Białynicki-Birula decomposition of Gr(l, V) in relation with that of $\mathbb{P}(\wedge^l V)$. Next, we prove our main result by giving a lower bound for the dimension of C for small prime characteristics. By applying Weyl's dimension

formula to calculate this lower bound, we conclude by proving Theorem 1.3 in Section 4.1.

Preliminaries

[0046] In this section we will introduce the most basic objects and notation for our paper. We recall that we will restrict to schemes of finite type defined over a fixed finite field $\mathbb{F}_q$.

[0047] For a positive integer $m \in \mathbb{Z}$, we will use the notation [m] to denote the finite set {1, . . . , m}. For $l \in [m]$, the set of all l-element subsets of [m] is denoted by

$$\binom{[m]}{l}.$$

We view

$$\binom{[m]}{l}$$

as a chain, where the total order is given by the lexicographic ordering. More precisely, we view the elements of

$$\binom{[m]}{l}$$

as increasing sequences of l-tuples of integers from [m], and we order them lexicographically. The lexicographic order on

$$\binom{[m]}{l}$$

will be denoted by $\preccurlyeq$ In particular, whenever

$$\binom{[m]}{l}$$

appears as an indexing set of some vector, we always assume that its elements are ordered according to $\preccurlyeq$. We will refer to an element of

$$\binom{[m]}{l}$$

as an l-subset.

[0048] An integer partition of m is a non-increasing sequence of positive numbers $\lambda=(\lambda_1, \ldots, \lambda_s)$ such that $\Sigma_{i=1}^{s}\lambda_i=m$. The Young diagram of λ is a top-left justified arrangement of the boxes with λ_i boxes in the i-th row. For example, the Young diagram of the integer partition $\lambda=(7, 3,3,2,1)$ of 16 is shown in FIG. **1**.

[0049] The coefficient of the monomial q^a in

$$\begin{bmatrix} m \\ l \end{bmatrix}_q$$

is given by the number of integer partitions of a whose Young diagram fit into an l×(m−l) grid. This well-known combinatorial fact is a direct consequence of the decomposition of the Grassmann variety $\mathrm{Gr}(l, \mathbb{F}_q^m)$ into Schubert cells, which we will review in the sequel. By abuse of notation, let us use $\lambda \subseteq l\times(m-l)$ to indicate that the Young diagram of the integer partition λ fits inside the l×(m−l) grid. Then we have the following polynomial identity which summarizes our discussion:

$$\begin{bmatrix} m \\ l \end{bmatrix}_q = 1 + \sum_{\lambda \subseteq l\times(m-l)} q^{\#\ of\ boxes\ in\ \lambda}.$$

[0050] Thus, the coefficients of the monomials $q^{l(m-l)}$ and $q^{l(m-l)-1}$ in

$$\begin{bmatrix} m \\ l \end{bmatrix}_q$$

are equal to 1. In particular, the leading term of

$$\begin{bmatrix} m \\ l \end{bmatrix}_q$$

is $q^{l(m-l)}$. We used this fact to justify (in the introduction) the fact that our codes in Theorem 4.1 satisfy the Singleton bound.

[0051] Let m=4, l=2. Then, there are 5 integer partitions whose Young diagram fits into 2×2 grid. We depicted the Young diagrams of these integer partitions in FIG. **2**.

[0052] It follows from the list of Young diagrams in FIG. **2** that

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = 1 + q + 2q^2 + q^3 + q^4.$$

[0053] We finish this subsection by introducing another commonly used notation. The multiplicative group of non-zero entries in $\mathbb{F}_q^{\times}$ will be denoted by $\mathbb{G}_m$.

2.1 The Grassmann Varieties

[0054] Let K be a field. Let SL_m denote the group of m×m matrices with determinant 1 with entries from K. The diagonal maximal torus in SL_m, denoted by T_m, is a split torus. The Borel subgroup of upper triangular matrices in SL_m, denoted by B_m, contains T_m. We denote by $X(T_m)$ the group of rational characters of T_m, and the dual of $X(T_m)$, that is $\mathrm{Hom}_{\mathbb{Z}}(X(T_m), \mathbb{Z})$, is denoted by $Y(T_m)$. The nondegenerate bilinear pairing between $X(T_m)$ and $Y(T_m)$ will be denoted by $\langle , \rangle$. The Weyl group of SL_m is isomorphic to S_m, the symmetric group of permutations of the set [m]. It acts on T_m by conjugation, hence, it acts on the groups $X(T_m)$ and $Y(T_m)$. However, the pairing $\langle , \rangle$ is S_m-invariant. The root system of the pair (SL_m, T_m) will be denoted by R. Explic-

itly, it is given by the set of vectors $R=\{\varepsilon_i-\varepsilon_j: 1\le i, j\le m\}$, where $\{\varepsilon_1, \ldots, \varepsilon_m\}$ is the standard basis for the m-dimensional Euclidean $\mathbb{Q}$-vector space. The system of positive roots determined by B_m, denoted by R^+, is given by $R^+=\{\varepsilon_i-\varepsilon_j: 1\le i<j\le m\}$. The subset of simple roots in R^+ will be denoted by S; it is given by $S=\{\alpha_i: \alpha_i=\varepsilon_i-\varepsilon_{i+1}, 1\le i\le m-1\}$. The duals of the basis vectors α_i $(1\le i\le m-1)$ are denoted by α_i^V, and the fundamental weights $\overline{\omega}_i$ $(1\le i\le m-1)$ are defined by equations

$$\langle \overline{\omega}_i, \alpha_j^\vee \rangle = \begin{cases} 1 & \text{if } i=j \\ 0 & \text{otherwise} \end{cases}$$

for $\alpha_j\in S$. Note that the i-th fundamental weight $\overline{\omega}_i$ is the highest weight vector of the i-th fundamental representation $\bigwedge^i k$ of SL_m. The submonoid generated by $\overline{w}_i$ $(1\le i\le m-1)$ in $X(T_m)$, denoted by $X(T_m)_+$, is the monoid of dominant weights. Then we have,

$$X(T_m)_+ = \{\lambda \in X(T_m) : \langle \lambda, \alpha_i^\vee \rangle \ge 0 \text{ for every } \alpha_i \in S\}.$$

[0055] It is well-known that for every finite dimensional irreducible representation W of SL_m, there is a unique dominant weight $\lambda\in X(T_m)_+$ called the highest weight of W. In other words, simple SL_m-modules are parametrized by the elements of $X(T_m)_+$.

[0056] Since it is the point of departure for our paper, we will briefly review the definition of the Plücker embedding. Let V be an m-dimensional vector space. We fix a basis $\{e_1, \ldots, e_m\}$ of V. Note that an l-dimensional subspace M of V can be identified with an l×m matrix A=A(M), where the rank of A is l. Indeed, the rows of such a matrix span an l-dimensional vector subspace; two such matrices A_1, A_2 span the same vector subspace if and only if there exists $g\in GL_l$ such that $A_1=gA_2$.

[0057] Let $Mat_{l,m}$ denote the space of l×m matrices (over a field) and let $Mat_{l,m}^0$ denote the Zariski open subset consisting of rank l matrices. Then GL_l acts by the left matrix multiplication on $Mat_{l,m}^0$, and the quotient is precisely the Grassmann variety Gr(l, V). In this interpretation, the elements of Gr(l, V) are the equivalence classes of matrices [A] where $A\in Mat_{l,m}^0$. The Plücker embedding of Gr(l, V) is defined by p: Gr(l, V)→

$$\mathbb{P}^{\binom{m}{l}-1}, [A] \mapsto (\det A_I)_{I\in\binom{[m]}{l}},$$

where A_I is the l×l-minor of A determined by the columns indexed by I.

[0058] Finally, let us point out the fact that Gr(l, V) is a homogeneous space for SL_m as well as for GL_m:

$$Gr(l, V) \cong SL_m/Stab_{SL_m}(\langle e_1, \ldots, e_l\rangle) \cong GL_m/Stab_{GL_m}(\langle e_1, \ldots, e_l\rangle).$$

[0059] Here, $\langle e_1, \ldots, e_l\rangle$ is the l-dimensional subspace spanned by $e_1, \ldots, e_l$ in V.

2.2 Projective Embeddings of Gr(l, V)

[0060] Let V denote the m-dimensional K-vector space K^m with the standard basis $\{e_1, \ldots, e_m\}$. The l-th fundamental representation of SL_m is given by the l-th exterior power of V. It is well-known that the Picard group of Gr(l, V) is generated by the ample line bundle $\mathcal{L}(\overline{\omega}_l)$.

[0061] The dual of the space of global sections, that is $H^0(Gr(l, V), \mathcal{L}(\overline{\omega}_l))^*$, is isomorphic to $\bigwedge^l V$. Therefore, the Plücker coordinates on Gr(l, V) are given by the restrictions of the coordinate functions on the affine space

$$\mathbb{A}^{\binom{m}{l}} \cong \bigwedge^l V.$$

[0062] Next, we will consider the space of global sections of the line bundle $\mathcal{L}(r\overline{\omega}_l)$, where r is a positive integer. Since $\mathcal{L}(r\overline{\omega}_l)$ is very ample, it gives a closed embedding,

$$\tau_r: Gr(l, V) \hookrightarrow \mathbb{P}\left(H^0(Gr(l, V), \mathcal{L}(r\overline{\omega}_l))^*\right). \tag{2.2}$$

[0063] The analogs of Plücker coordinates for (2.2) are called the standard monomials. In this section, we will compute the parameters of the codes that we will construct from (2.2). Since the underlying idea of computations is the same for every r>1, we will present the simplest case, that is r=2.

[0064] To identify the projective space in (2.2), we first embed Gr(l, V) into $\mathbb{P}^s\times\mathbb{P}^s$, where

$$s = \binom{m}{l} - 1;$$

this embedding is given by the composition of the diagonal embedding of Gr(l, V) into Gr(l, V)×Gr(l, V) followed by the doubled Plücker embedding. Then we use the Segre embedding to embed the doubled projective space into a bigger projective space. We denote the morphism defined by these compositions by ι. In summary, we have the following diagram:

$$\iota: Gr(l, V) \xrightarrow{diag} Gr(l, V)\times Gr(l, V) \xrightarrow{p\times p} \mathbb{P}^s\times\mathbb{P}^2 \xrightarrow{Segre} \mathbb{P}^{s^2+2s}, \tag{2.3}$$

[0065] We will describe explicitly the image of (2.3).

[0066] Let M be a point from Gr(l, V), and let $(m_1, m_2, \ldots, m_{s+1})$ denote its image under the Plücker embedding. Then we have

$$\iota: M \xrightarrow{diag} (M, M) \xrightarrow{(p,p)} ((m_1, \ldots, m_{s+1}), (m_1, \ldots, m_{s+1})) \xrightarrow{Segre} (m_i m_j)_{\substack{i=1,\ldots,s+1\\ j=1,\ldots,s+1}}. \tag{2.4}$$

[0067] Equivalently

$$(m_i m_j)_{\substack{i=1,\ldots,s+1 \\ j=1,\ldots,s+1}}$$

is the point that is represented by the tensor product M⊗M in $\mathbb{P}(\wedge^l V \otimes \wedge^l V)$.

[0068] We will show that ι is very useful for understanding the embedding (2.2). We proceed with some general remarks.

[0069] Let G be a connected reductive group, and let B be a Borel subgroup. Let P be a standard parabolic subgroup, that is, P is a parabolic subgroup and $B \subset P$. We assume that all of these (sub)groups are defined over $K := \mathbb{F}_q$.

[0070] There is a canonical projection map π: G/B→G/P, and for every locally free sheaf $\mathcal{S}$ on G/P, there is an isomorphism

$$H^0(G/P, \mathcal{S}) \to H^0(G/B, \pi^*\mathcal{S}). \tag{2.5}$$

[0071] In our special case, if P is the maximal parabolic subgroup in $G=SL_m$ corresponding to the fundamental weight $\overline{\omega}_l$, and B is the Borel subgroup B_m, then we have the isomorphism

$$H^0(G/P, \mathcal{L}(r\varpi_l)) \to H^0(G/B, \pi^*\mathcal{L}(r\varpi_l)) \tag{2.6}$$

for every $r \in \mathbb{Z}_+$. Therefore, as far as our embedding (2.2) concerned, we can work with the SL_m module $H^0(G/B, \pi^*\mathcal{L}(r\overline{\omega}_l))$. To be precise, we will work with the dual of this module.

[0072] Let T be a maximal torus such that $T \subset B$. For every $\lambda \in X(T)$, we will use the abbreviation $H^0(r\overline{\omega}_l) := H^0(G/P, \mathcal{L}(r\overline{\omega}_l))$. If λ is a dominant weight from $X(T)_+$, then the G-module, $V(\lambda) := H^0(-w_0\lambda)^*$, where w_0 is the longest element of the Weyl group W, is called the Weyl module associated with λ.

[0073] Thus, the following may be understood:

[0074] The formal characters of V(λ) and $H^0(\lambda)$ are always equal.

[0075] In characteristic 0, Weyl modules give irreducible representations of G, and furthermore, V(λ) is isomorphic to $H^0(\lambda)$. However, in characteristic $p \neq 0$, they (the Weyl modules) are in general non-simple. Nevertheless, the isomorphism $V(\lambda) \cong H^0(\lambda)$ holds if V(λ) is simple. In this case, we can compute the dimension of V(λ) via Weyl character formula. Since this is a formal computation, it can be performed over $\mathbb{Z}$ (hence over $\mathbb{C}$) as well.

[0076] For every field K and positive integer $m \in \mathbb{N}$, the exterior powers $\wedge^l K^m$ ($1 \leq l \leq m$) are simple SL_m-modules. More generally, (over a finite field $K = \mathbb{F}_q$) there is an explicit characterization of the weights λ such that V(λ) is simple. It goes as follows: Let p denote the characteristic of K, and let ρ denote the weight $\overline{\omega}_1 + \ldots + \overline{\omega}_{m-1}$. Then V(λ) is simple over K if and only if for each positive root $\alpha = \varepsilon_i - \varepsilon_j \in R^+$ with $1 \leq i < j \leq m$ the following property holds: Let $\langle \lambda+\rho, \alpha^V \rangle = ap^s + bp^{s+1}$, where a, b, s are nonnegative integers such that $0 < a < p$. Then there should exist $\beta_0, \beta_1, \ldots, \beta_b \in R^+$ with $\langle \lambda+\rho, \beta_i^V \rangle = p^{s+1}$ for $1 \leq i \leq b$ and $\langle \lambda+\rho, \beta_0^V \rangle = ap^s$ with $\alpha = \Sigma_{i=0}^{b} \beta_i$ and with $\alpha - \beta_0 \in R$. Equivalently, there exist integers $i = i_0 < i_1 < \ldots < i_b < i_{b+1} = j$ such that $\{\beta_i : 0 \leq i \leq b\} = \{\varepsilon_{i_v} - \varepsilon_{i_{v+1}} : 0 \leq v \leq b\}$ and $\beta_0 \in \{\varepsilon_i - \varepsilon_{i_1}, \varepsilon_{i_b} - \varepsilon_j\}$. Notice that for every sufficiently big prime number, we have b=s=0, hence, $\langle \lambda+\rho, \alpha^V \rangle = a < p$. In this case, all of the subsequent conditions automatically hold. Therefore, V(λ) is a simple SL_m (K)-module.

2.3 Schubert Varieties in Gr(l, V)

[0077] Let G be an algebraic group and let B be a Borel subgroup of G. Let G/P be a projective homogeneous space, where P is a parabolic subgroup such that $B \subseteq P$. To a large extent, the geometry and the topology of G/P is determined by its Schubert subvarieties. By definition, a Schubert variety in G/P is the Zariski closure of a B-orbit in G/P. In the case of Grassmann varieties, they can be defined quite explicitly.

[0078] For a subset $J \subset [m]$, we will denote by E_J the subspace $\langle e_j : j \in J \rangle$. In particular, we will denote by $E_{[j]}$ ($j \in [m]$) the subspace $\langle e_1, \ldots, e_j \rangle$. Let $I = \{i_1, \ldots, i_l\}$ be an element of

$$\binom{[m]}{l}.$$

The Schubert cell associated with I in Gr(l, V) is the affine space

$$C_I := \{W \in Gr(l, V) : \dim(W \cap E_{[j]}) = |I \cap [j]| \text{ for every } j \in [m]\}. \tag{2.11}$$

[0079] It is not difficult to verify that if I≠I', then $C_I \cap C_{I'} = \emptyset$. It is also not difficult to check that the union of all Schubert cells is equal to Gr(l, V). The decomposition

$$Gr(l, V) = \bigsqcup_{I \in \binom{[m]}{l}} C_I \tag{2.12}$$

is called the Bruhat-Chevalley decomposition of Gr(l, V).

[0080] The Zariski closure of C_I in Gr(l, V), called the Schubert variety associated with I, is given by

$$X_I := \overline{C_I} = \{W \in Gr(l, V) : \dim(W \cap E_{[j]}) \geq |I \cap [j]| \text{ for every } j \in [m]\}.$$

[0081] The intersection ring (the Chow ring) of Gr(l, V) is completely determined by the classes of Schubert varieties. For $I = \{i_1, \ldots, i_l\}$, $J = \{j_1, \ldots, j_l\}$ from

$$\binom{[m]}{l},$$

the inclusion relationship between X_I and X_J is given by the entry-wise comparisons:

$$X_I \subseteq X_J \Leftrightarrow i_r \leq j_r \text{ for every } r \in [l]. \tag{2.13}$$

[0082] We have an example of the Hasse diagram of this partial order in FIG. **4**.

[0083] It is not difficult to check from (2.13) that the Schubert cell $C_{\{m-l+1, m-l+2, \ldots, m\}}$ is open and dense in Gr(l, V), and that, there is a unique one-codimensional Schubert subvariety X' in Gr(l, V). The indexing set of X' is given by {m−l, m−l+2, m−l+3, . . . , m}. This divisor of Gr(l, V) is precisely the intersection of the image of the Plücker embedding (FIG. **3**) with the hypersurface of $\mathbb{P}(\wedge^l V)$ that is given by the vanishing of the last coordinate variable with respect to $\preccurlyeq$. This remark will be justified in Section 4.

2.4 Tsfasman-Serre Theorem

[0084] In this section, to simplify our notation and to be consistent with our references, we will denote by π_m the q-analog of m+1, where q is a power of a prime number. In other words, we set

$$\pi_m := [m+1]_q = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q.$$

[0085] If X is a variety defined over $\mathbb{F}_q$, then by $X(\mathbb{F}_q)$ we will denote the set of $\mathbb{F}_q$-rational points of X.

[0086] As we mentioned before in our discussion of the Grassmann varieties, π_m is the cardinality of the projective space $\mathbb{P}^m(\mathbb{F}_q)$.

[0087] Theorem 2.15 Let P be a nonzero homogeneous polynomial of degree r from $\mathbb{F}_q[x_0, \ldots, x_m]$. If r≤q+1, then

$$|\{x \in \mathbb{P}^m(\mathbb{F}_q) : P(x) = 0\}| \leq rq^{m-1} + \pi_{m-2}. \tag{2.16}$$

[0088] Let $a_1, \ldots, a_r$ be distinct elements of $\mathbb{F}_q$. If r≤q, then it is easy to check that the polynomial

$$G_r(x_0, \ldots, x_m) := (x_1 - a_1 x_0) \ldots (x_1 - a_r x_0)$$

[0089] has exactly $rq^{m-1}+\pi_{m-2}$ zeros in $\mathbb{P}^m(\mathbb{F}_q)$. Likewise, it is easy to check that the polynomial

$$g_r(x_1, \ldots, x_m) = (x_1 - a_1) \ldots (x_1 - a_r),$$

[0090] has exactly rq^{m-1} zeros in $\mathbb{A}^m(\mathbb{F}_q)$. It is well-known that this is the maximum of the number of $\mathbb{F}_q$-rational points on a hypersurface of degree r in $\mathbb{A}^m(\mathbb{F}_q)$.

3. Some Helpful Lemmas

[0091] In this section, K denotes a finite field with q elements; all of our algebraic groups are defined over K.

[0092] Let s denote

$$\binom{m}{l} - 1,$$

and let $\{F_1, \ldots, F_{s+1}\}$ denote the standard basis for $\wedge^l V$; if r∈{1, . . . , s+1} corresponds to the subset

$$I = \{i_1, \ldots, i_l\} \in \binom{[m]}{l},$$

then F_r is given by $F_r = e_{i_1} \wedge \ldots \wedge e_{i_l}$. Let $x_1, \ldots, x_{s+1}$ denote the corresponding Plücker coordinate functionals on $\wedge^l V$. Thus, $x_r = F^*_r$ for r∈{1, . . . , r+1}. Then the coordinate functionals on $\mathbb{P}(\wedge^l V \otimes \wedge^l V)$ are given by $x_i \otimes x_j$, i, j∈{1, . . . , s+1}.

[0093] As we mentioned before, we know from Nogin's work that the minimum distance on Gr(l, V) is given by

$$d = |\{M \notin H_v : M \in Gr(l, V)\}| = q^{l(m-l)}, \tag{3.1}$$

[0094] where v is any completely decomposable vector from $\wedge^{m-l} V \cong (\wedge^l V)^*$, and H_v is the hypersurface defined by $H_v = \{w \in \wedge^l V : w \wedge v = 0\}$ (see). Here, a vector $v \in \wedge^{m-l} V$ is said to be completely decomposable if there exist m−l vectors $u_1, \ldots, u_{m-l} \in V$ such that $v = u_1 \wedge \ldots \wedge u_{m-l}$. It is easy to check that the Plücker coordinate functions are completely decomposable. In the sequel, we will not distinguish between $\wedge^{m-l} V$ and $(\wedge^l V)^*$.

[0095] We set v to be the last Plücker coordinate function with respect to $\preccurlyeq$, that is, $v := x_{s+1}$. Let us write $[H_v]$ for the projectivization of H_v, that is, the image of H_v under the canonical projection $(\wedge^l V)\setminus\{0\} \to \mathbb{P}(\wedge^l V)$. Then $[H_v] \cap Gr(l, V)$ is the unique Schubert divisor of Gr(l, V). Thus, we have the following alternative description of d:

$$d = |\{M \in Gr(l, V) : x_{s+1}(M) \neq 0\}| \tag{3.2}$$

$$= \binom{m}{l}_q - |\{M \in Gr(l, V) : x_{s+1}(M) = 0\}|.$$

[0096] It follows from our discussion in Subsection 2.3 that d is the number of K-rational points on the open the subset $\{M \in Gr(l, V) : x_{s+1}(M) \neq 0\}$. From a similar vein, we will compute the minimum distance of the embedding $Gr(l, V) \hookrightarrow \mathbb{P}(H^0(r\overline{\omega}_l)^*)$. The main "novel ingredient" of our computation is the fact that the geometry of a higher twisting of the Plücker embedding is essentially determined by the cellular decomposition of the relevant projective space.

[0097] The action of GL_m on V induces an action on $\wedge^l V$. Let $\lambda: \mathbb{G}_m \to T_m$ denote the one-parameter subgroup defined by

$$\lambda(t) = \mathrm{diag}(t^{v_0}, \ldots, t^{v_{n-1}}), \tag{3.3}$$

[0098] where $v_0, \ldots, v_{m-1}$ are integers such that $v_i = 2^{v_{i+1}}$ for i∈{0, . . . , m−2}. By λ, we get an action of $\mathbb{G}_m$ on $\mathbb{P}(\wedge^l V)$:

$$t \cdot [A] := [\lambda(t) \cdot A] \quad (t \in \mathbb{G}_m, A \in \wedge^l V). \tag{3.4}$$

[0099] The notation [A] indicates that we are taking the image of the vector A under the projection $\wedge^l V\setminus\{0\} \to \mathbb{P}(\wedge^l V)$. This should not be confused with [m], which

stands for the set {1, . . . , m}. We trust that this clash of notation will not cause any confusion for the reader.

[0100] Lemma 3.5. The fixed point set of the action of $\mathbb{G}_m$ is given by $\mathbb{P}(\wedge^l V))^{\mathbb{G}_m}=\{[F_1], \ldots, [F_{s+1}]\}$.

[0101] Let $[(a_0, \ldots, a_s)]$ be a point in $\mathbb{P}(\wedge^l V)$, and let $t\in \mathbb{G}_m$. Then we have

$$t\cdot[(a_0, \ldots, a_s)] = \left[\left(t^{\sum_{i=0}^{l-1} v_i} a_0, \ldots, t^{\sum_{i=m-l}^{m-1} v_i} a_s\right)\right] \quad (t \in \mathbb{G}_m).$$

[0102] The way that we chose the positive integers $v_0, \ldots, v_{m-1}$ ensures that the exponents of t in on the right hand side of (3.6) are strictly decreasing from left to right. It follows that

$$[(a_0, \ldots, a_s)] \neq \left[\left(t^{\sum_{i=0}^{l-1} v_i} a_0, \ldots, t^{\sum_{i=m-l}^{m-1} v_i} a_S\right)\right], \tag{3.6}$$

[0103] unless all but one of the coordinates is zero. Therefore, the fixed point set of the $\mathbb{G}_m$-action is given by {[(1,0, . . . , 0)], [(0,1,0, . . . , 0)], . . . , [(0, . . . , 0,1)]}, which is precisely our standard basis $\{F_1, \ldots, F_{s+1}\}$.

[0104] For $i\in\{1, \ldots, s+1\}$, the subvariety

$$F_i^+ := \{(a_1, \ldots, a_i, 1, 0, \ldots, 0) : a_1, \ldots, a_i \in K\} \subset \mathbb{P}(\wedge^l V) \tag{3.7}$$

[0105] is called the plus-cell corresponding to F_i; it is isomorphic to the affine space K^i. Since $\mathbb{P}(\wedge^l V)=\bigsqcup_{i=0}^{m} F_i^+$, the plus-cell decomposition is a cellular decomposition of $\mathbb{P}(\wedge^l V)$ in the sense of algebraic topology.

[0106] Clearly, the Grassmann variety Gr(l, V) in $\mathbb{P}(\wedge^l V)$ is stable under the action (3.4), and furthermore, every fixed point of λ is contained in Gr(l, V). It follows that the intersections of the plus-cells (3.7) with Gr(l, V) gives the plus-cell decomposition of Gr(l, V).

[0107] Next, we will prove that this plus-cell decomposition of the Grassmann variety agrees with its Bruhat-Chevalley decomposition, (2.12).

[0108] Lemma 3.8 Let $r\in\{0, \ldots, s\}$ correspond to the subset $I\in \binom{[m]}{l}$ with respect to $\preccurlyeq$. Then $F_r^+\cap$Gr(l, V) is equal to the Schubert cell C_I.

[0109] The Plücker embedding is a GL_m-equivariant morphism. Let B_m denote the Borel subgroup of upper triangular matrices in GL_m. On one hand we have that C_I is the B_m-orbit of F_r. On the other hand, we see that the B_m-orbit of [(0, . . . ,0,1,0, . . . ,0)], where 1 appears in the r-th position, is given by F_r^+. Indeed, the action of B_m on $\mathbb{P}(\wedge^l V)$ is obtained from the first fundamental representation of GL_m on $V\cong K^m$, whereby, $B_m\cdot e_r=\langle e_1, \ldots, e_r\rangle$. Since the nonzero Plücker coordinate functions on F_r^+ are the ones that correspond to the l-subsets $J\in \binom{[m]}{l}$ such that $J\preccurlyeq I$, we see the B_m-orbit of F_r in $\mathbb{P}(\wedge^l V)$ is contained in F_r^+. In particular, we see that $F_r^+\cap$Gr(l, V)=$B_m\cdot F_r$. This finishes the proof of our lemma.

[0110] The unique Schubert divisor $X_{\{m-l,m-l+2, \ldots, m\}}$ is equal the intersection of Gr(l, V) with the hypersurface $\{x_{s+1}=0\}$ of $\mathbb{P}(\wedge^l V)$.

[0111] As we already pointed out above, the uniqueness of the one-codimensional Schubert subvariety is easy to check from the Bruhat-Chevalley order (2.13). The Plücker coordinate function x_{s+1} corresponds to the subset {m−l+1, . . . , m} which is maximal with respect to $\preccurlyeq$. In other words, by Lemma 3.8, $\{x_{s+1}\neq 0\}\cap$Gr(l, V) is the open Schubert cell in Gr(l, V). Therefore, its complement, also called the boundary, is B_m-stable. In particular, the boundary of the open cell is a union of Schubert subvarieties. Since there is a unique codimension one Schubert subvariety (hence, all other proper Schubert subvarieties are contained in this one), the boundary is equal to $X_{\{m-l,m-l+2, \ldots, m\}}$ as claimed. But the complement is equal to the intersection $\{x_{s+1}=0\}\cap$Gr(l, V). This finishes the proof of our claim.

4. The Main Theorem

[0112] Recall that the dimension of an algebraic geometric $[n, k, d]_q$-code C on a projective variety $X\hookrightarrow \mathbb{P}^r$ is given by the "dimension" of the image of the evaluation map ev: $E^*\to \mathbb{F}_q^n$, that is, l=m−dimker(ev). Here, we view E^* as the vector space homogeneous linear forms on $\mathbb{P}^r=\mathbb{P}(E)$. If the projective embedding of X is E is an equivariant embedding with respect to an action of an affine group G, then the kernel of the evaluation map has the structure of a finite dimensional G-module. In the case of Grassmann codes that we discussed earlier, the Plücker embedding of Gr(l, V) is given by the SL_m-representation $\wedge^l V$, which is well-known to be a simple SL_m-module, hence, the corresponding evaluation map is injective. This is essentially the reason why one does not need to mention anything further about l; it is simply the dimension of the irreducible representation $\wedge^l V$. However, for all other projective embeddings of Gr(l, V), the kernel of the evaluation map is not trivial since the corresponding SL_m-module may not be simple. In general, the simpleness of the corresponding Weyl module strongly depends on the characteristic of the base field $\mathbb{F}_q$.

[0113] We are now ready to prove our main theorem.

[0114] Theorem 4.1. Let C denote the projective [n, k, d]-system associated with the closed embedding obtained from the composition

$$\iota: Gr(l, V) \to \mathbb{P}\left(\bigwedge^r\left(\bigwedge^l V\right)\right) \to \mathbb{P}\left(\left(\bigwedge^l V\right)^{\otimes r}\right).$$

[0115] Then the parameters of C satisfy

1. $n = \begin{bmatrix} m \\ l \end{bmatrix}_q$,
2. $q^{l(m-l)} - rq^{l(m-l)-1} \leq d \leq q^{l(m-l)} - (r-1)q^{l(m-l)-1}$,
3. $\dim soc_{SL_m}(H^0(r\overline{\omega}_l)) \leq k \leq dim H^0(r\overline{\omega}_l)$,

[0116] where $soc_{SL_m} H^0(r\overline{\omega}_l)$ is the unique simple submodule of $H^0(r\overline{\omega}_l)$. Moreover, the upper bound for k is achieved if $H^0(r\overline{\omega}_l)$ is a simple SL_m-module.

[0117] Before we give the proof of our main theorem, we have the following observations.

[0118] First, let us point out that if the characteristic of the underlying field is big enough, then $H^0(r\overline{\omega}_l)$ is a simple SL_m-module. In this case, we have $k=\dim H^0(r\overline{\omega}_l)$. As we will show in the sequel, the dimension of $H^0(r\overline{107}_l)$ can be

calculated by the well-known Weyl dimension formula. These observations show that Theorem 1.3 follows from Theorem 4.1 when p is sufficiently big.

[0119] Secondly, even if $H^0(r\overline{\omega}_l)$ is not simple, in lower ranks, the formal character of $\mathrm{soc}_{SL_n}(H^0(r\overline{\omega}_l))$, hence its dimension, are not so difficult to compute.

[0120] By our discussion from Subsection 2.2, the image of ι is contained in the projective subspace $\mathbb{P}(H^0(r\overline{\omega}_l)^*)$ in $\mathbb{P}((\wedge^l V)^{\otimes r})$; for r=2, the corresponding embedding of Gr(l, V) is explicitly given by the assignment (2.4). The case of an arbitrary $r\in\mathbb{N}$ is a straightforward generalization of this special case. Also, we already know that the number of $\mathbb{F}_q$-rational points of Gr(l, V) is

$$\begin{bmatrix} m \\ l \end{bmatrix}_q.$$

This is the length of our code. We now proceed to compute the minimum distance.

[0121] Let $\mathcal{O}_{\mathbb{P}((\wedge^l V)^{\otimes r})}(1)$ denote the first Serre twist of the structure sheaf of $\mathbb{P}((\wedge^l V)^{\otimes r})$. The pullback of this line bundle under the Segre embedding is equal to the r-fold tensor product $\mathcal{O}_{\mathbb{P}(\wedge^l V)}(1)\boxtimes\ldots\boxtimes\mathcal{O}_{\mathbb{P}(\wedge^l V)}(1)$. The restriction of this product to the diagonal, which is isomorphic to $\mathbb{P}(\wedge^l V)$, is given by the multiplication of the sections of the factors; it lands in $\mathcal{O}_{\mathbb{P}(\wedge^l V)}(r)$. Therefore, we notice that a degree one hypersurface in $\mathbb{P}((\wedge^l V)^{\otimes r})$ determines a degree r hypersurface in $\mathbb{P}(\wedge^l V)$. Since our goal is to compute the minimum distance, we will work with the hypersurfaces in $\mathbb{P}((\wedge^l V)^{\otimes r})$ having the highest number of $\mathbb{F}_q$-rational points. Therefore, we will consider the following degree r polynomial:

$$P := x_{s+1}(x_{s+1}-b_1x_s)\ \ldots\ (x_{s+1}-b_{r-1}x_s)\in\mathbb{F}_q[x_{i_1}\ \ldots\ x_{i_r}: 1\le i_1\le\ \ldots\ \le i_r\le s+1],$$

[0122] where $b_1,\ldots,b_{r-1}$ are distinct nonzero elements of $\mathbb{F}_q$. In particular, the number of $\mathbb{F}_q$-rational points of the hypersurface $U_P:=\{P=0\}$ in $\mathbb{P}(\wedge^l V)$ is equal to $rq^{s-1}+\pi_{s-2}$.

[0123] Next, we intersect U_P with the Grassmann Gr(l, V); we will determine the number of $\mathbb{F}_q$-rational points of the intersection. In other words, we want to determine the number

$$\left|\{M\in Gr(l,V): (x_{s+1}(x_{s+1}-b_1x_s)\ \ldots\ (x_{s+1}-b_{r-1}x_s))(M)=0\}\right|. \quad (4.4)$$

[0124] We split our analysis of the defining equation in (4.4) into three major cases:

1. $x_{s+1}(M)=x_s(M)=0$ and $M\in Gr(l,V)$;
2. $x_{s+1}(M)=0$, $x_s(M)\neq 0$ and $M\in Gr(l,V)$;
3. $x_{s+1}(M)\neq 0$, $((x_{s+1}-b_1x_s)\ \ldots\ (x_{s+1}-b_{r-1}x_s))(M)=0$, and $M\in Gr(l,V)$.

[0125] In the first case, that is $\{M\in\mathbb{P}(\wedge^l V): x_{s+1}(M)=x_s(M)=0\}\cap Gr(l,V)$, we get every point M from Gr(l, V) which is not contained in the Schubert cells of codimension ≤1. Since Gr(l, V) has a unique Schubert divisor, we see that

$$\left|\left\{M\in\mathbb{P}\left(\wedge^l V\right): x_{s+1}(M)=x_s(M)=0\right\}\cap Gr(l,V)\right| = \begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l}? - q^{l(m-l)-1}.$$

? indicates text missing or illegible when filed

[0126] In the second case, we get precisely the codimension one Schubert cell in Gr(l, V), which has $q^{l(m-l)-1}$ elements. Finally, in the third case, the intersection

$$\left\{M\in\mathbb{P}\left(\wedge^l V\right): x_{s+1}(M)\neq 0,\ ((x_{s+1}-b_1x_s)\ \ldots\ (x_{s+1}-b_{r-1}x_s))(M)=0\right\}\cap Gr(l,V)$$

[0127] is a hypersurface in the dense Bruhat cell of Gr(l, V). Since the defining equation of this hypersurface is given by $(x_{s+1}(M)-b_1x_s)\ldots(x_{s+1}(M)-b_{r-1}x_s)=0$, where $x_{s+1}(M)\neq 0$, and b_i's are distinct elements from $\mathbb{F}_q$, this hypersurface has exactly $(r-1)q^{l(m-l)-1}$ $\mathbb{F}_q$-rational points. Thus, we see that the total number of zeros of the homogeneous polynomial $x_{s+1}(x_{s+1}-b_1x_s)\ldots(x_{s+1}-b_{r-1}x_s)$ on Gr(l, V) is given by

$$\left(\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} - q^{l(m-l)-1}\right) + q^{l(m-l)} + (r-1)q^{l(m-l)-1} = \begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} + (r-1)q^{l(m-l)-1}.$$

[0128] It follows that an upper bound for the minimum distance on Gr(l, V) in $\mathbb{P}((\wedge^l V)^{\otimes r})$ is given by

(4.3)

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - \left(\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} + (r-1)q^{l(m-l)-1}\right) = q^{l(m-l)} - (r-1)q^{l(m-l)-1}. \quad (4.5)$$

[0129] Next, we will prove our formula for the lower bound for the minimum distance. To this end, let Q be a homogeneous degree r polynomial from $\mathbb{F}_q[x_1,\ldots,x_{s+1}]$ such that the intersection $H_Q\cap Gr(l,V)$ attains the maximum number of $\mathbb{F}_q$-rational points among all such intersections. Here, H_Q denotes the hypersurface in $\mathbb{P}(\wedge^l V)$ defined by Q. It follows that the intersection of H_Q with the open cell of

Gr(l, V) is nonempty. We assume that this intersection attains the maximum number $rq^{l(m-l)-1}$. Under these assumptions, we see that

$$|H_Q \cap Gr(l, V)|_{\mathbb{F}_q} \leq rq^{l(n-l)-1} + \begin{bmatrix} m \\ l \end{bmatrix} - q^{l(m-l)}, \tag{4.6}$$

[0130] where

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)}$$

is the number of $\mathbb{F}_q$-rational points in the complement of the open cell in the Grassmannian. Since (4.6) is an upper bound for the number of zeros of Q on Gr(l, V) over $\mathbb{F}_q$, a lower bound for the minimum distance is given by

$$\begin{bmatrix} m \\ l \end{bmatrix}_q - \left(\begin{bmatrix} m \\ l \end{bmatrix}_q - q^{l(m-l)} + rq^{l(m-l)-1} \right) = q^{l(m-l)} - rq^{l(m-l)-1}. \tag{4.7}$$

[0131] By combining (4.5) and (4.7), we obtain the following inequalities for the minimum distance,

$$q^{l(m-l)} - rq^{l(m-l)-1} \leq d \leq q^{l(m-l)} - (r-1)q^{l(m-l)-1}. \tag{4.8}$$

[0132] It remains to compute the dimension of our code. Since the image of $\mathbb{Z}$ is contained in $\mathbb{P}((H^0(Gr(l, V), \mathcal{L}(r\overline{\omega}_l))^*)$, the image of the evaluation map ev: $((\wedge^l V)^{\otimes r})^* \to \mathbb{F}_q^n$ agrees with the image of the (restricted) evaluation map ev: $H^0(r\overline{\omega}_l)^* \to \mathbb{F}_q^n$. On one hand, if $H^0(r\overline{\omega}_l)$ is a simple SL_m-module, then so is $H^0(r\overline{\omega}_l)^*$. In this case, the kernel of the evaluation map is trivial, hence, $k=\dim H^0(r\overline{\omega}_l)$. On the other hand, if our finite dimensional module $H^0(r\overline{\omega}_l)$ is not simple, then it is not guaranteed that the kernel of the evaluation map is trivial. Nevertheless, it is always true that the sum of all simple submodules, namely, the socle of $H^0(r\overline{\omega}_l)$, is not contained in the kernel. Indeed, it is well-known that $\mathrm{soc}_{SL_m} H^0(r\overline{\omega}_l)$ is simple, so, if it were contained in the kernel, then the evaluation map has to map the whole vector space to 0, which would be absurd. This argument shows that the dimension of the evaluation map is at least as big as $\dim \mathrm{soc}_{SL_m} H^0(r\overline{\omega}_l)$. Hence, the proof of our assertion is finished.

[0133] We conclude this subsection by a remark that expands on the last part of the proof of our Theorem 4.1. Let λ denote the (dominant) weight $r\overline{\omega}_l$. We assume that $H^0(\lambda)$ is a simple SL_m-module. Then, as we pointed out above, the Weyl module $V(\lambda)$ is isomorphic to $H^0(\lambda)$. Since $V(\lambda)$ is generated, as an SL_m-module, by a B-stable line of weight λ, we see that the SL_m-orbit of a nonzero vector in the socle of $H^0(\lambda)^*$ generates the whole module. In our case, the SL_m-orbit of a nonzero vector on such a line is isomorphic to Gr(l, V). Thus, the projective space on $H^0(\lambda)^*$ is spanned by the image of the embedding of our Grassmann variety.

4.1 Weyl's Character and Dimension Formulas

[0134] Let $\lambda=r\overline{\omega}_l$ ($r\in\mathbb{N}$) be a dominant weight for SL_m. As we mentioned before, assuming that $H^0(r\overline{\omega}_l)$ is simple, its character and dimension can be computed as if we are working over the field of complex numbers. In particular, in this case we can apply the well-known combinatorics of Young tableaux. The purpose of this subsection is to briefly explain how this methodology works. A general reference for this material is.

[0135] Recall that the monoid of dominant weights for (SL_m, B_m, T_m) is generated by the fundamental weights $\overline{\omega}_i$ ($1\leq i\leq m-1$). Let $a_1\overline{\omega}_1+\ldots+a_{m-1}\overline{\omega}_{m-1}\in X(T_m)_+$ be a dominant weight for some nonnegative integers $a_i\in\mathbb{N}$ ($1\leq i\leq m-1$), and set $\lambda_m:=0$. Then the sequence $\lambda=(\lambda_1, \ldots, \lambda_m)$ defined by the equations,

$$\lambda_i - \lambda_{i+1} = a_i \text{ for } i \in [m-1]$$

[0136] is an integer partition, that is, $\lambda_1\geq\lambda_2\geq\ldots\geq\lambda_m$. Clearly, if we are given λ, then we can solve these equations for a_i's as well. In other words, there is a one-to-one correspondence between the integer partitions and the dominant weights for the special linear groups. In light of this bijection, $a_1\overline{\omega}_1+\ldots+a_{m-1}\overline{\omega}_{m-1} \leftrightsquigarrow \lambda$, hereafter, for the sake of brevity, let us denote by $W(\lambda)$ the simple module $H^0(Gr(l, V), \mathcal{L}(a_1\overline{\omega}_1+\ldots+a_{m-1}\overline{\omega}_{m-1}))^*$.

[0137] Let $\lambda=(\lambda_1, \ldots, \lambda_m)$ be an integer partition. Recall that the Young diagram of λ is a top-left justified arrangement of the boxes with λ_i boxes in the i-th row. A semistandard Young tableau of shape λ (or an SSTY of shape λ, for short) is a filling of the boxes of the Young diagram of shape λ with positive integers that is weakly increasing in every row and strictly increasing in every column. For example, in FIG. **5**, we have an SSYT of shape (5,4,4).

[0138] Let T be an SSYT of shape λ. Let us define the weight of T as the monomial $x^T:=x_{i_1}^{n_1}\ldots x_{i_k}^{n_k}$, where the integer i_j ($1\leq j\leq k$) appears in T n_j times. Then the character of a simple SL_m ($\mathbb{C}$)-module $W(\lambda)$ is given by the Schur function $s_\lambda(x_1, \ldots, x_m)$ which is defined as the weight generating function of all SSYT of shape λ,

$$s_\lambda(x_1, \ldots, x_m) = \sum_{T:SSTY\ of\ shape\ \lambda} x^T.$$

[0139] In particular, by specializing the variables x_i ($1\leq i\leq n$) to 1, we get the dimension of $W(\lambda)$,

[0140] $\dim W(\lambda)$=#SSYT of shape λ filled with entries from $\{1, \ldots, m\}$.

[0141] This number can be calculated in a combinatorial way by the hook length formula. To explain this formula, we first put coordinates on the boxes of the Young diagram of $\lambda=(\lambda_1, \ldots, \lambda_m)$ by identifying it with the set $\{(i, j): j\in[\lambda_i], i\in[m]\}$. For example, the coordinates of the integer partition (5,4,3) are depicted in FIG. **6**.

[0142] The content of a box u=(i, j) in the Young diagram of λ is defined as c(u):=j−i. The hook length of u, denoted by h(u) is defined as the number of boxes directly to the right of u and directly below u, counting u itself once. The diagram on the left (FIG. **7**A) shows the contents and the diagram on the right (FIG. **7**B) shows the hook lengths of the boxes of λ.

[0143] In this notation we have the following concrete form of the Weyl's dimension formula,

$$s_\lambda(1, \ldots, 1) = \prod_{u \in \text{Young diagram of } \lambda} \frac{m + c(u)}{h(u)}. \tag{4.9}$$

[0144] Let V be a three dimensional vector space over $\mathbb{C}$. Let l=2. In this case, the partition corresponding to the dominant weight $\overline{\omega}_l$ is λ=(1,1), and therefore, we have the following SSYT tableaux for the irreducible representation $W(\lambda) \cong H^0(Gr(2, V), \mathcal{L}(\overline{\omega}_2))$:

1	1	2
2	3	3

[0145] Note that, corresponding to each SSYT of shape λ, there is a Plücker coordinate function. For the tableaux in the above example, the Plücker coordinate functions are given by p_{12}, p_{13}, and p_{23}. In particular, we have

$$dim W(\lambda) = dim H^0(Gr(2, V), \mathcal{L}(\varpi_2)) = 3.$$

[0146] The partition corresponding to $2\overline{\omega}_2$ is given by λ=(2,2). Thus, the SSYT's corresponding to the "Plücker coordinates" of the embedding for the line bundle $\mathcal{L}(2\overline{\omega}_2)$ are listed in FIG. **8**. In particular, we see that $H^0(Gr(2, \mathbb{C}^3), \mathcal{L}(2\overline{\omega}_2))$ is six dimensional. Of course, we can get the same count by using formula in (4.9).

[0147] Before we describe an application of this combinatorics to our main theorem, let us point out, by our running example, that for every sufficiently big characteristic p>0, the $SL_m(\mathbb{F}_q)$-module $H^0(r\omega_l)$ is simple.

[0148] For SL_3, ρ denotes $\overline{\omega}_1+\overline{\omega}_2$. Then $2\overline{\omega}_2+\rho=\overline{\omega}_1+3\overline{\omega}_2$. By definition, the fundamental dominant weight $\overline{\omega}_i$ is the dual of the coroot α_i^V. Therefore, we have

$$\langle \varpi_1 + 3\varpi_2, \alpha_1^V \rangle = 1,$$
$$\langle \varpi_1 + 3\varpi_2, \alpha_2^V \rangle = 3,$$
$$\langle \varpi_1 + 3\varpi_2, (\alpha_1 + \alpha_2)^V \rangle = 4.$$

[0149] For every prime characteristic p≥5, the SL_3 (F_q)-module W(λ) is simple.

[0150] Corollary 4.13 For every sufficiently big prime characteristic p, the dimension of the code C defined in Theorem 4.1 is given by

$$dim H^0(r\varpi_l) = \frac{\prod_{i=0}^{l-1} (m-i)^{(r)}}{\prod_{i=1}^{l} (i)^{(r)}}. \tag{4.14}$$

[0151] We know that for every sufficiently big prime characteristic, the SL_m-module $H^0(r\omega_l)$ is simple. Theorem 4.1 implies that the dimension of our code is given by the Weyl's dimension formula. The integer partition $\lambda=(\lambda_1, \ldots, \lambda_m)$ that corresponds to the dominant weight $r\overline{\omega}_l$ is given by

$$\lambda_1 = \ldots = \lambda_l = r \text{ and } \lambda_j = 0 \text{ for } j \in \{l+1, \ldots, m\}.$$

[0152] The contents and the hook lengths of the boxes of λ are depicted in FIGS. **9**A and **9**B.

[0153] To finish the proof, we will use the formula in (4.9) by using the content and hook length tableaux that are shown in (4.5). To keep track of the products, we multiply the entries row-by-row, from top-to-bottom. We multiply the entries of the rows of the content tableau from left-to-right:

$$\text{Row 1: } m \cdot (m+1) \ \ldots \ (m+r-1) = m^{(r)},$$
$$\text{Row 2: } (m-1) \cdot m \ \ldots \ (m+r-2) = (m-1)^{(r)},$$
$$\vdots$$
$$\text{Row } l\text{: } (m-(l-1)) \cdot (m-(l-2)) \ \ldots \ (m-(l-r)) = (m-(l-1))^{(r)}.$$

[0154] Thus, the numerator of the hook length formula is given by $\Pi_{i=0}^{l-1}(m-i)^{(r)}$. For the hook length tableau, we multiply the entries of the rows from right-to-left:

$$\text{Row 1: } l \cdot (l+1) \ \ldots \ (l+r-1) = l^{(r)},$$
$$\text{Row 2: } (l-1) \cdot l \ \ldots \ (l+r-2) = (l-1)^{(r)},$$
$$\vdots$$
$$\text{Row } 1\text{: } 1 \cdot 2 \ \ldots \ r = (1)^{(r)}.$$

[0155] Then the denominator of the hook length formula is given by $\Pi_{i=0}^{l-1}(1+i)^{(r)}$. This finishes the proof of our corollary.

[0156] We choose a sufficiently large prime characteristic p so that $H^0(r\omega_l)$ is a simple SL_m-module. Then the dimension k of our code is equal to $dim H^0(r\omega_l)$. Hence, our theorem follows from Theorem 4.1 and Corollary 4.13.

[0157] We consider the embedding associated with the highest weight $2\overline{\omega}_3$ of the Grassmann variety $Gr(3, \mathbb{F}_q^5)$, where the characteristic of $\mathbb{F}_q$ is sufficiently large so that $H^0(2\overline{\omega}_3)$ is a simple SL_5-module. Then the parameters of our code are given by

$$n = \begin{bmatrix} 5 \\ 3 \end{bmatrix}_q = \frac{[5]_q[4]_q[3]_q}{[3]_q[2]_q[1]_q} = 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6,$$
$$k = \frac{5^{(2)}4^{(2)}3^{(2)}}{1^{(2)}2^{(2)}3^{(2)}} = \frac{5 \cdot 6 \cdot 4 \cdot 5 \cdot 3 \cdot 4}{1 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 4} = 50,$$
and
$$q^6 - 2q^5 \le d \le q^6 - q^5.$$

[0158] Note that, if q>3, then n−d is significantly bigger than k=50.

[0159] Construction of Quantum Error correcting codes from Higher Grassmann codes

[0160] We first extend the Higher Grassmann codes to the case where the degree v of the polynomials is no longer bounded above by q, but by (q−1)l(m−l). This is necessary for the construction of quantum codes. Then we obtain the

following extensions of the results considered earlier and these are discussed in the sequel to the original paper that also has been accepted for publication in the same journal.

[0161] Theorem 0.1 The dimension of the higher Grassmann code on $Gr(F_q)$ of degree ν, where $0\leq\nu<(q-1)l(m-l)$, is given by the formula:

$$dim C_{Gr}(F_q)(\nu)=\sum_{0\leq t\leq\nu,\ t\equiv\nu \bmod q-1}\ \sum_{r=1}^{\min\{t,l(m-l)\}} h(r,m,l)g(t,r,q-1),$$

where

$$h(r,m,l)=\sum_{c=0}^{r}(-1)^{r-c}r_c\left[\prod_{i=1}^{m-l}\prod_{j=1}^{c}\prod_{s=1}^{m-l}\frac{i+j+s-1}{i+j+s-2}\right],$$

and

$$g(t,r,q-1)=\sum_{j=0}^{\left\lfloor\frac{t-r}{q-1}\right\rfloor}(-1)^j\binom{l}{j}\binom{t-1-(q-1)j}{r-1}.$$

[0162] Theorem 0.2 Let $0\leq\nu\leq(q-1)l(m-l)-1$. If μ is defined by the equation $\mu:=(q-1)(l(m-l)-1)-\nu$, then the dual of $C_{Gr(F_q)}(\nu)$ is given by one of the following two cases:

$$C_{Gr(F_q)}(\nu)^{\perp}=\begin{cases}C_{Gr(F_q)}(\mu) & \text{if } \nu\neq 0 \bmod(q-1),\\ \overline{C_{Gr(F_q)}(\mu)} & \text{if } \nu=0 \bmod(q-1)\end{cases}.$$

[0163] where $C_{Gr(F_q)}(\mu)$ is the code obtained from $C_{Gr(F_q)}(\mu)$ by adding the code word that is 1 everywhere.

[0164] Theorem 0.3 Let $C_{Gr(l,V)}(\nu)$ denote the q-ary degree ν Higher Grassmann code on Gr(l, V). Let r and s denote non-negative integers defined by $\nu-1=r(q-1)+s$, where $0\leq s<q-1$. If $\nu<(q-1)l(m-l)$, then the minimum distance of $C_{Gr(l,V)}(\nu)$ is bounded as follows:

$$(q-s)q^{l(m-l)-r-1}\leq d\leq(q-1-s)q^{l(m-l)-r-1}.$$

[0165] We will next outline two different constructions of quantum error correcting codes based on the higher Grassmann codes. The construction of quantum codes from these Projective Reed-Muller codes has been well understood at least for over a decade. This invokes certain construction of quantum codes starting with a pair of classical codes, commonly referred to as the Calderbank-Shor-Steane construction. We proceed to discuss in some detail, how similar constructions apply to the Higher Grassmann codes to produce quantum codes. We will also point out that the resulting quantum codes have certain advantages over the quantum codes produced from the Projective Reed-Muller codes.

[0166] With reference to FIG. **10**, a key idea of our construction of quantum codes from the Higher Grassmann codes is to first show that one can imbed the Higher Grassmann codes as sub-codes of the Projective Reed-Muller codes.

[0167] In a first construction we start with the Grassmann variety imbedded into a projective space using what is called the Plücker imbedding and follow it by imbedding the above projective space in a much larger projective space ($\mathbb{P}^m$) as in our paper. This corresponds to the ample line bundle $\mathcal{O}(\nu)$ on our Grassmann variety: in this construction we do not put any restriction on how large ν can be. Moreover we start with two line bundles $\mathcal{O}(\nu_1)$ and $\mathcal{O}(\nu_2)$, with $\nu_2=\nu_1+k(q-1)$, where $\mathbb{F}_q$ denotes the finite field of cardinality q over which we choose to work and $k>0$ is an integer. The global sections of the above two line bundles correspond to homogeneous polynomials over $\mathbb{F}_q$ in m+1 variables of degrees ν_1 and ν_2, respectively. The corresponding higher Grassmann codes are obtained by evaluating these sections at the $\mathbb{F}_q$-rational points on the Grassmann variety. We obtain two higher Grassmann codes this way, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ with $C_{Gr}(\nu_1)\subseteq C_{Gr}(\nu_2)$. Moreover the minimum distance of the code $C_{Gr}(\nu_2)-C_{Gr}(\nu_1)\geq$the minimum distance of the code $C_{Gr}(\nu_2)$: further we have recently calculated the minimum distances of these higher Grassmann codes extending the calculations in which only handled the case where the degrees ν_1, and ν_2 were assumed to be no larger than q.

[0168] On applying the CSS construction to the two higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$, we obtain quantum error correcting codes whose parameters are determined by the parameters of the higher Grassmann codes as follows: the length of the code will be the number of $\mathbb{F}_q$-rational points on the Grassmannian, the dimension of the resulting quantum code is the difference of the dimensions of the two Grassmann codes $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$, and the minimum distance is bounded below by the minimum of the minimum distance of the code $C_{Gr}(\nu_2)$ and the minimum distance of the code $C_{Gr}(\nu_1)^{\perp}$.

[0169] Advantages of such quantum codes. First the dimensions of the higher Grassmann codes $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ are much larger (in fact, several times larger) than the corresponding Grassmann codes as the calculation of the dimension of the higher Grassmann codes in shows. In view of the calculation of the dimensions of the resulting quantum codes as above, this advantage also shows up in the dimensions of the resulting quantum codes. A comparison of the minimum distance of the higher Grassmann codes with the minimum distances of the corresponding Projective Reed-Muller code shows that the minimum distances for the higher Grassmann codes are typically much larger: this translates into much larger minimum distances for the resulting quantum codes as well. Moreover, larger dimensions and larger minimum distances translate into codes that perform much better.

[0170] Another advantage is that, as there is no restriction on the degrees ν_1 and ν_2, we obtain large families of quantum codes this way.

[0171] In a second construction we restrict to line bundles $\mathcal{O}(\nu)$ so that $1\leq\nu\leq\lfloor\ell(m-\ell)(q-1)/2\rfloor$ and $2\nu\equiv 0 \bmod(q-1)$. Then our first observation is that corresponding higher Grassmann code $C_{Gr}(\nu)$ is self-dual. Moreover, in this case one can write $\nu^{\perp}=\ell(m-\ell)(q-1)-\nu$, as $k(q-1)+\nu$, where $k=\ell(m-\ell)-(2\nu/(q-1))$. Therefore, this fits into the framework of the first case with $\nu_1=\nu$ and $\nu_2=\nu^{\perp}=\ell(m-\ell)(q-1)-\nu$. The construction in 1, then produces quantum codes, whose length and dimension are as in case 1 above and where the minimum distance is given by the minimum distance of the dual code $C_{Gr}(\nu)^{\perp}$. Note: it is again here that we need to determine the min distance of the duals of the higher Grassmann codes.

[0172] Advantages of the resulting quantum codes: These codes share several of the features of the quantum codes in 1, and hence their advantages.

Implementation Details

[0173] We will start with a pair of Higher Grassmann codes, C_1 and C_2, with C_2 a subcode of C_1. Then denoting the parity check matrices for the codes C_1 and C_2 by $H(C_1)$ and $H(C_2)$, the resulting quantum code produced by invoking the CSS construction is a stabilizer code where the stabilizer matrix is given by

$$S = \begin{pmatrix} H(C_2^{\perp}) & 0 \\ 0 & H(C_1) \end{pmatrix},$$

[0174] where $H(C_1)$ ($H(C_2^{\perp})$) denotes the parity check matrix of the Higher Grassmann code C_1 ($C_2^{\perp}$), with $C_2^{\perp}$ denoting the dual of the code C_2.

[0175] Therefore, it is possible to invoke the circuitry for encoding and decoding quantum stabilizer codes as shown in FIG. **11**, which illustrates a circuit having a structure of an [[n; k; d]] stabilizer code. A quantum data register $|\psi\rangle_D=|\psi_1\psi_2 \ldots \psi_k\rangle$ is entangled with redundancy qubits $|0\rangle_R=|0_1 0_2 \ldots 0_{n-k}\rangle$ via an encoding operation to create a logical qubit $|\psi\rangle_L$. After encoding, a sequence of n−k stabilizer checks P_i are performed on the register, and each result copied to an ancilla qubit A_i. The subsequent measurement of the ancilla qubits provides an m-bit syndrome.

[0176] FIG. **12** illustrates a general procedure for active recovery in a quantum error correction code. The logical qubit $|\psi\rangle_L$ of an [[n, k, d]] stabilizer code is subject to an error process E. A generating set of stabilizers S are measured on the logical state to yield an m-bit syndrome $\mathcal{S}$. This syndrome is processed by a decoder to determine the best recovery operation $\mathcal{R}$ to return the logical state to the codespace. After the recovery has been applied, the output of the error correction cycle is $\mathcal{R}E|\psi\rangle_L$. Double lines indicate classical information flow.

[0177] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims. The present disclosure is capable of other implementations and of being practiced or carried out in various ways.

[0178] It must also be noted that, as used in the specification and the appended claims, the singular forms "a," "an" and "the" include plural referents unless the context clearly dictates otherwise. Ranges may be expressed herein as from "about" or "approximately" one particular value and/or to "about" or "approximately" another particular value. When such a range is expressed, other exemplary implementations include from the one particular value and/or to the other particular value.

[0179] By "comprising" or "containing" or "including" is meant that at least the named compound, element, particle, or method step is present in the composition or article or method, but does not exclude the presence of other compounds, materials, particles, method steps, even if the other such compounds, material, particles, method steps have the same function as what is named.

[0180] In describing example implementations, terminology will be resorted to for the sake of clarity. It is intended that each term contemplates its broadest meaning as understood by those skilled in the art and includes all technical equivalents that operate in a similar manner to accomplish a similar purpose. It is also to be understood that the mention of one or more steps of a method does not preclude the presence of additional method steps or intervening method steps between those steps expressly identified. Steps of a method may be performed in a different order than those described herein without departing from the scope of the present disclosure. Similarly, it is also to be understood that the mention of one or more components in a device or system does not preclude the presence of additional components or intervening components between those components expressly identified.

We claim:

1. An apparatus to encode and decode quantum [[n; k; d]] stabilizer codes, comprising:

an encoder that entangles a quantum data register $|\psi\rangle_D=|\psi_1\psi_2 \ldots \psi_k\rangle$ with redundancy qubits $|0\rangle_R=|0_1 0_2 \ldots 0_{n-k}\rangle$ to create a logical qubit $|\psi\rangle_L$; and

stabilizer check logic that, after encoding, performs a sequence of n−k stabilizer checks P_i on the quantum data register and that copies each result to an ancilla qubit A_i,

wherein the subsequent measurement of the ancilla qubits provides an m-bit syndrome.

2. The apparatus of claim **1**, wherein the redundancy qubits comprise higher Grassmann codes.

3. The apparatus of claim **2**, wherein a Grassmann variety is imbedded into a projective space using Plücker imbedding that is imbedded in a higher-order projective space ($\mathbb{P}^m$) that corresponds to line bundles $\mathcal{O}(\nu)$ on the Grassmann variety.

4. The apparatus of claim **3**, wherein there is a no restriction on how large ν is, wherein two line bundles $\mathcal{O}(\nu_1)$ and $\mathcal{O}(\nu_2)$ are used with $\nu_2=\nu_1+k(q-1)$, wherein $\mathbb{F}_q$ denotes a finite field with q elements, where q is a power of a prime number, p and wherein k>0 is an integer.

5. The apparatus of claim **4**, wherein the higher Grassmann codes are obtained by evaluating global sections of the two line bundles correspond to homogeneous polynomials over $\mathbb{F}_q$ in m+1 variables of degrees ν_1 and ν_2, respectively, at the $\mathbb{F}_q$-rational points on the Grassmann variety.

6. The apparatus of claim **5**, wherein two higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ with $C_{Gr}(\nu_1)\subseteq C_{Gr}(\nu_2)$ are obtained, and

wherein a CSS construction is applied to the two higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ to obtain quantum error correcting codes whose parameters are determined by the parameters of the higher Grassmann codes as follows: the length of the code will be the number of $\mathbb{F}_q$-rational points on the Grassmannian, the dimension of the resulting quantum code is the difference of the dimensions of the two Grassmann codes $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$, and the minimum distance is bounded below by the minimum of the minimum distance of the code $C_{Gr}(\nu_2)$ and the minimum distance of the code $C_{Gr}(\nu_1)^{\perp}$.

7. The apparatus of claim **3**, wherein the line bundles $\mathcal{O}(\nu)$ are restricted such that $1\leq\nu\leq\lfloor \ell(m-\ell)(q-1)/2\rfloor$ and $2\nu\equiv 0 \bmod (q-1)$.

8. The apparatus of claim **7**, wherein the higher Grassmann codes $C_{Gr}(\nu)$ are self-dual.

9. The apparatus of claim **8**, wherein $\nu^{\perp}=\ell(m-\ell)(q-1)-\nu$, as $k(q-1)+\nu$, where $k=\ell(m-\ell)-(2\nu/(q-1))$, and wherein

a CSS construction is applied to the higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ to obtain quantum error correcting codes whose parameters are determined by the parameters of the higher Grassmann codes as follows: the length of the code will be the number of $\mathbb{F}_q$-rational points on the Grassmannian, the dimension of the resulting quantum code is the difference of the dimensions of the two Grassmann codes $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$, and the minimum distance is bounded below by the minimum of the minimum distance of the code $C_{Gr}(\nu_2)$ and the minimum distance of the code $C_{Gr}(\nu_1)^{\perp}$.

10. A method to encode and decode quantum [[n; k; d]] stabilizer codes error correcting codes from higher Grassmann codes, comprising:

generating higher Grassmann codes that are imbedded as sub-codes of in a higher-order projective space ($\mathbb{P}^m$) that corresponds to line bundles $\mathcal{O}(\nu)$ on the Grassmann variety;

entangling a quantum data register $|\psi\rangle_D=|\psi_1\psi_2 \ldots \psi_k\rangle$ with redundancy qubits $|0\rangle_R=|0_1 0_2 \ldots 0_{n-k}\rangle$ that use the higher Grassmann codes to create a logical qubit $|\psi\rangle_L$;

performing a sequence of n−k stabilizer checks P_i on the quantum data register and copying each result to an ancilla qubit A_i; and

performing a subsequent measurement of the ancilla qubits to provide an m-bit syndrome.

12. The method of claim **11**, further comprising placing no restrictions on how large ν is and using two line bundles $\mathcal{O}(\nu_1)$ and $\mathcal{O}(\nu_2)$ with $\nu_2=\nu_1+k(q-1)$, wherein $\mathbb{F}_q$ denotes a finite field with q elements, where q is a power of a prime number, p and wherein k>0 is an integer.

13. The method of claim **12**, further comprising obtaining the higher Grassmann codes by evaluating global sections of the two line bundles correspond to homogeneous polynomials over $\mathbb{F}_q$ in m+1 variables of degrees ν_1 and ν_2, respectively, at the $\mathbb{F}_q$-rational points on the Grassmann variety.

14. The method of claim **13**, wherein two higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ with $C_{Gr}(\nu_1)\subseteq C_{Gr}(\nu_2)$ are obtained, and further comprising: applying a CSS construction to the two higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ to obtain quantum error correcting codes whose parameters are determined by the parameters of the higher Grassmann codes as follows: the length of the code will be the number of $\mathbb{F}_q$-rational points on the Grassmannian, the dimension of the resulting quantum code is the difference of the dimensions of the two Grassmann codes $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$, and the minimum distance is bounded below by the minimum of the minimum distance of the code $C_{Gr}(\nu_2)$ and the minimum distance of the code $C_{Gr}(\nu_1)^{\perp}$.

15. The method of claim **10**, wherein the line bundles $\mathcal{O}(\nu)$ are restricted such that $1\leq\nu\leq\lfloor \ell(m-\ell)(q-1)/2\rfloor$ and $2\nu\equiv 0 \bmod (q-1)$.

16. The method of claim **15**, wherein the higher Grassmann codes $C_{Gr}(\nu)$ are self-dual.

17. The method of claim **16**, wherein $\nu^{\perp}=\ell(m-\ell)(q-1)-\nu$, as $k(q-1)+\nu$, where $k=\ell(m-\ell)-(2\nu/(q-1))$, and further comprising applying a CSS construction to the higher Grassmann codes, $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$ to obtain quantum error correcting codes whose parameters are determined by the parameters of the higher Grassmann codes as follows: the length of the code will be the number of $\mathbb{F}_q$-rational points on the Grassmannian, the dimension of the resulting quantum code is the difference of the dimensions of the two Grassmann codes $C_{Gr}(\nu_1)$ and $C_{Gr}(\nu_2)$, and the minimum distance is bounded below by the minimum of the minimum distance of the code $C_{Gr}(\nu_2)$ and the minimum distance of the code $C_{Gr}(\nu_1)^{\perp}$.

18. A method for active recovery in a quantum error correction code, comprising

performing an error process E on a logical qubit $|\psi\rangle_L$ of an [[n, k, d]] stabilizer code;

measuring a generating set of stabilizers S on a logical state to yield an m-bit syndrome $\mathcal{S}$; and

processing the m-bit syndrome $\mathcal{S}$ by a decoder to determine a best recovery operation $\mathcal{R}$ to return the logical state to a codespace,

wherein after the recovery operation has been applied, the output of an error correction cycle is $\mathcal{R}E|\psi\rangle_L$.

* * * * *