Downloaded from orbit.dtu.dk on: Apr 27, 2024

DTU Library

Point-line incidence on Grassmannians and majority logic decoding of Grassmann codes

Beelen, Peter; Singh, Prasant

Published in:
Finite Fields and Their Applications

Link to article, DOI:
10.1016/j.ffa.2021.101843

Publication date:
2021

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):
Beelen, P., & Singh, P. (2021). Point-line incidence on Grassmannians and majority logic decoding of Grassmann codes. *Finite Fields and Their Applications*, *73*, Article 101843. https://doi.org/10.1016/j.ffa.2021.101843

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

POINT-LINE INCIDENCE ON GRASSMANNIANS AND MAJORITY LOGIC DECODING OF GRASSMANN CODES

PETER BEELEN AND PRASANT SINGH

Abstract. In this article, we consider the decoding problem of Grassmann codes using majority logic. We show that for two points of the Grassmannian, there exists a canonical geodesic between these points once a complete flag is fixed. These geodesics are used to construct a large set of parity checks orthogonal on a coordinate of the code, resulting in a majority decoding algorithm.

1. Introduction

Let q be a prime power and let $\mathbb{F}_q$ be a finite field with q elements. The Grassmannian $G_{\ell,m}$ is an algebraic variety whose points correspond to ℓ-dimensional subspaces of a fixed m dimensional space over $\mathbb{F}_q$. Corresponding to a projective variety, one can associate a linear code in a natural way using the points of the variety as a projective system [27]. The codes $C(\ell, m)$ associated in this way to the Grassmannians $G_{\ell,m}$ are known as Grassmann codes. Grassmann codes were first studied by Ryan [23, 24] over the binary field and later by Nogin [19] over any finite field. There it was shown that $C(\ell, m)$ is a q-ary $[n, k, d]$ code where

$$n = \begin{bmatrix} m \\ \ell \end{bmatrix}_q, \ k = \binom{m}{\ell}, \text{ and } d = q^{\ell(m-\ell)}, \tag{1}$$

where $\left[\begin{smallmatrix} m \\ \ell \end{smallmatrix}\right]_q$ is the Guassian binomial coefficient given by

$$\begin{bmatrix} m \\ \ell \end{bmatrix}_q := \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-\ell+1}-1)}{(q^\ell-1)(q^{\ell-1}-1)\cdots(q-1)}.$$

These codes have been an object of study ever since they were discovered. For example, Nogin [19, 20] determined the weight distribution of the Grassmann codes $C(2, m)$ and $C(3, 6)$. Kaipa, et al. [12] determined the weight distribution of the Grassmann code $C(3, 7)$. Several initial and final generalized Hamming weights of $C(\ell, m)$ are known as well [8, 9, 19]. Also variants of Grassmann codes, called affine Grassmann codes, obtained by only taking the points in an affine part of the Grassmann variety in the projective system, have been studied [1].

However, as far as the efficient decoding of Grassmann codes is concerned, not much is known apart from an approach using permutation decoding [10, 14] leading to an algorithm capable of correcting up to $d/\binom{m}{\ell} - 1$ errors. In this article we give

Date: December 18, 2020.

a decoding algorithm for Grassmann codes $C(\ell, m)$ based on (one-step) majority logic decoding. A key ingredient is that the dual Grassmann code $C(\ell, m)^{\perp}$ is a linear code of minimum distance three. Using ingredients from [2], it was shown in [3], that the weight three parity checks generate $C^{\perp}$. This gives the Grassmann code $C(\ell, m)$ an LDPC-like structure and majority logic decoding is a method used for example in [15, Ch. 17] to correct errors for such codes. Moreover, majority logic decoding has been used to give a decoding algorithm for binary Reed–Muller codes [16, Th. 20, Ch. 13.7], which can be seen as special cases of affine Grassmann codes. In this article we study to which extent one-step majority logic decoding can be used for Grassmann codes. In order to do this, we construct sets of parity checks orthogonal on every coordinate of the code. An essential ingredient in this construction, is the study of geodesics between points on the Grassmannian, which forms an important part of this paper. Finally we show that the resulting decoder can correct approximately up to $d/2^{\ell+1}$ errors for a fixed ℓ, and q tending to infinity. For a fixed ℓ and q, and m tending to infinity, we can correct up to $M_q(\ell)d/2^{\ell+1}$ errors, where

$$M_q(\ell) := \begin{cases} \prod_{i=1}^{\ell} \frac{q^i}{q^i-1} & \text{if } q \text{ is even,} \\ \\ \prod_{i=1}^{\ell-1} \frac{q^i(q-1)}{q^{i+1}-1} & \text{if } q \text{ is odd.} \end{cases} \tag{2}$$

This performance compares favourably to previously known efficient decoders for $C(\ell, m)$, see Remark 4.8 for details.

2. Preliminaries

We begin this section with recalling the definitions of Grassmann varieties. We give the construction of Grassmann codes, linear codes associated to Grassmann varieties and recall the parameters of these codes. We define what we call a line in Grassmannians and state a result that classify all these lines in terms of linear subspaces of the vector space. For the sake of completeness, we recall some notions and results related to lines in Grassmannian and Grassmann codes. These are the results that we will be using in next two sections of this article.

As in the introduction, let $\mathbb{F}_q$ be a finite field with q elements where q is a prime power and let $V = \mathbb{F}_q^m$ be the vector space over $\mathbb{F}_q$ of dimension m. Let $\ell \leq m$ be a positive integer. The Grassmannian $G_{\ell,m}$ of all ℓ-planes of V is defined by

$$G_{\ell,m} := \{P \subseteq V : \ P \text{ is a subspace of V and } \dim P = \ell\}.$$

Note that, when $\ell = 1$, the Grassmannian $G_{1,m}$ is the projective space $\mathbb{P}^{m-1} = \mathbb{P}^{m-1}(\mathbb{F}_q)$. In general, the Grassmannian $G_{\ell,m}$ can be embedded into a projective space $\mathbb{P}^{\binom{m}{\ell}-1}$ via the Plücker map. More precisely, let $\mathbb{I}(\ell, m)$ be the set defined by

$$\mathbb{I}(\ell, m) = \{\alpha = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{Z}^\ell : \ 1 \leq \alpha_1 < \cdots < \alpha_\ell \leq m\}. \tag{3}$$

Fix some total order on $\mathbb{I}(\ell,m)$ and for every point $P \in G_{\ell,m}$, let M_P be an $\ell \times m$ matrix whose rows forms a basis of P. The Plücker map is the map

$$Pl : G_{\ell,m} \to \mathbb{P}^{\binom{m}{\ell}-1} \text{ defined by } P \mapsto [p_\alpha(M_P)]_{\alpha\in\mathbb{I}(\ell,m)}$$

where the α^{th}coordinate, $p_\alpha(M_P)$, is the minor of the $\ell \times \ell$ matrix obtained from M_P by selecting its ℓ columns indexed by the coordinates of α. It is well known that the Plücker map Pl is a well-defined, injective map. Moreover, the image of the Grassmannian $G_{\ell,m}$ is a projective algebraic subset of $\mathbb{P}^{\binom{m}{\ell}-1}$. It is not hard to see that the cardinality of the Grassmannian $G_{\ell,m}$ is given by the Gaussian binomial coefficient $\begin{bmatrix} m \\ \ell \end{bmatrix}_q$. Further, $G_{\ell,m} \subset \mathbb{P}^{\binom{m}{\ell}-1}$ can be defined as the set of common zeroes of the Plücker polynomials, which are certain irreducible quadratic polynomials. It is well known that the Plücker map embeds $G_{\ell,m}$ non-degenerately into $\mathbb{P}^{\binom{m}{\ell}-1}$. In other words, $G_{\ell,m}$ does not lie on any hyperplane in $\mathbb{P}^{\binom{m}{\ell}-1}$. Moreover, using duality one can see that $G_{\ell,m}$ and $G_{m-\ell,m}$ are isomorphic varieties. Therefore we will assume throughout in this article that $\ell \leq m-\ell$. For a more detailed description of Grassmannians and their properties, we refer to [13, 17].

Note that, from the Schubert cell decomposition of Grassmannians [17, 3.2.3] and [11, Thm.1], we have

$$|G_{\ell,m}| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q = \sum_{\beta\in\mathbb{I}(\ell,m)} q^{\delta(\beta)}, \tag{4}$$

where, $\delta(\beta) = \sum_{i=1}^{\ell}(\beta_i - i)$ for every $\beta = (\beta_1, \ldots, \beta_\ell) \in \mathbb{I}(\ell,m)$.

Grassmann codes can now be defined using the points of $G_{\ell,m}$, or more precisely its image under the Plücker embedding, as a projective system. Some authors use another point of view when constructing Grassmann codes, which we briefly describe now for the convenience of the reader. Let $G_{\ell,m} = \{P_1, P_2, \ldots, P_n\}$, , where $n = \begin{bmatrix} m \\ \ell \end{bmatrix}_q$. For $1 \leq i \leq n$, choose an $\ell \times m$ matrices M_i, whose rowspace is P_i. Now let $\mathbf{X} = (X_{ij})$ be an $\ell \times m$ matrix in variables X_{ij}. For any $\alpha \in \mathbb{I}(\ell,m)$, let X_α be the minor of the $\ell \times \ell$ submatrix of $\mathbf{X}$ obtained by selecting its columns indexed by $\alpha_1, \alpha_2, \ldots, \alpha_\ell$. Finally, let $\mathbb{F}_q[X_\alpha : \alpha \in \mathbb{I}(\ell,m)]_1$ be the vector space spanned by the minors X_α. Consider the evaluation map

$$\mathrm{Ev} : \mathbb{F}_q[X_\alpha : \alpha \in \mathbb{I}(\ell,m)]_1 \to \mathbb{F}_q^n \text{ defined by } f \mapsto c_f = (f(M_1), \ldots, f(M_n)).$$

The map is well defined as the Grassmannian $G_{\ell,m}$ does not lie on a hyperplane [17, Exercise 3.1.2]. The image of this evaluation map is exactly the Grassmann code $C(\ell,m)$. Indeed, where using the point of view of projective systems, one constructs the columns of a generator matrix of the code $C(\ell,m)$, the evaluation map produces all linear combinations of the rows of this generator matrix and hence all codewords of $C(\ell,m)$.

From the construction it is clear that the coordinates of a codeword of $C(\ell,m)$ can be indexed by the points of $G_{\ell,m}$. Therefore, we can interpret the support of

a codeword $c \in C(\ell, m)$ as a set consisting of points from $G_{\ell,m}$. To be precise, if $c = c_f \in C(\ell, m)$ is any codeword then we write the support of c as

$$\mathrm{Supp}(c) = \{P_i \in G_{\ell,m} : f(M_i) \neq 0\}.$$

In the same way, the support of a codeword from $C(\ell, m)^{\perp}$ will be viewed as a subset of $G_{\ell,m}$.

Later we will need that the automorphism group of a Grassmann code $C(\ell, m)$ acts transitively on the set of coordinates. This follows easily, since $\mathrm{GL}(m, \mathbb{F}_q)$ acts transitively on the set of ℓ-dimensional subspaces of V. For a full description of the automorphism group of $C(\ell, m)$, see [7, Th. 3.7], [25, Exercise 3.5] and [5, Sec 6.6].

Now, let us describe *lines* in $G_{\ell,m}$, which we will use extensively in the next sections [21, Ch. 3.1].

Definition 2.1. Let $U \subset W$ be two subspaces of V of dimensions $\ell - 1$ and $\ell + 1$ respectively. A line in $G_{\ell,m}$ is define by

$$L(U, W) := \{P \in G_{\ell,m} : U \subset P \subset W\}.$$

It is well known that the Plücker image of $L(U, W)$ gives a line in the projective space $\mathbb{P}^{\binom{m}{\ell}} - 1$. Further, every line of projective space $\mathbb{P}^{\binom{m}{\ell}-1}$ contained in $G_{\ell,m}$ is the Plücker image of some $L(U, W)$ [6, Lemma 5, Page 57]. Here, we are identifying the Grassmannian $G_{\ell,m}$ and its image under Plücker map. The next lemma is a simple consequence of the definition of a line on the Grassmannian.

Lemma 2.2. [9, Lemma 3] *Let P and Q be two distinct points of the Grassmannian $G_{\ell,m}$. The following are equivalent:*

(1) P and Q lie on a line in $G_{\ell,m}$,
(2) $\dim(P \cap Q) = \ell - 1$,
(3) $\dim(P + Q) = \ell + 1$.

Dually, it is also not hard to determine whether or not two distinct lines intersect.

Lemma 2.3. *Let $L(U_1, W_1)$ and $L(U_2, W_2)$ be two distinct lines on the Grassmannian $G_{\ell,m}$. Then these two lines intersect if and only if one of the following is satisfied:*

(1) $U_1 = U_2$ and $\dim(W_1 \cap W_2) = \ell$,
(2) $W_1 = W_2$ and $\dim(U_1 + U_2) = \ell$,
(3) $U_1 \neq U_2$, $W_1 \neq W_2$, and $U_1 + U_2 = W_1 \cap W_2$.

In first two cases, the intersection point is $W_1 \cap W_2$, $U_1 + U_2$ respectively. In the third case the intersection point is $U_1 + U_2$ (which equals $W_1 \cap W_2$).

Proof. It is not hard to see that if (1), (2), or (3) is satisfied, then the lines $L(U_1, W_1)$ and $L(U_2, W_2)$ intersect in the indicated point. Conversely, suppose that $L(U_1, W_1)$ and $L(U_2, W_2)$ intersect. In this case there exist an ℓ-dimensional space P satisfying

$U_1 \subset P \subset W_1$ and $U_2 \subset P \subset W_2$. If $U_1 \neq U_2$ and $W_1 \neq W_2$, then $U_1 + U_2 \subseteq P \subseteq W_1 \cap W_2$, but equality needs to hold as $\dim(U_1 + U_2) \geq \ell \geq \dim(W_1 \cap W_2)$. □

The following notion of injection distance between two points $P, Q \in G_{\ell,m}$ is defined in [26, Def. 2].

Definition 2.4. Let $P, Q \in G_{\ell,m}$ be given. The injection distance between P and Q is defined by $\mathrm{dist}(P, Q) := \ell - \dim(P \cap Q)$.

In particular Lemma 2.2 implies that two distinct points of the Grassmannian lie on a line if and only if they are at distance one. In the next lemma we quote a result from [4] in which the number of points at distance i from a given point P was determined.

Lemma 2.5. [4, Lemma 9.3.2] *Let $P \in G_{\ell,m}$ be given. For any $0 \leq i \leq \ell$ the cardinality of the set $\{Q \in G_{\ell,m} : \mathrm{dist}(P, Q) = i\}$ is given by*

$$q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q.$$

For future reference, we state and prove the following lemma, where an alternative expression for the cardinality of $\{Q \in G_{\ell,m} : \mathrm{dist}(P, Q) = i\}$ is given:

Lemma 2.6. *For any $1 \leq i \leq \ell$ the following identity holds:*

$$\sum_{\substack{\ell \geq r_1 > \cdots > r_i \geq 1 \\ 1 \leq s_1 < \cdots < s_i \leq m-\ell}} \prod_{j=1}^{i} q^{\ell+i-r_j+s_j-1} = q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q.$$

Proof. Let $\mathcal{R}(i, \ell)$ be the set of all i-tuples $\mathbf{r} = (r_1, \ldots, r_i) \in \mathbb{Z}^i$ satisfying $\ell \geq r_1 > \cdots > r_i \geq 1$. Similarly, let $\mathbb{I}(i, m-\ell)$ be the set defined in equation (3). Further, write $a_j = \ell - r_j + 1$ and $\mathbf{a} = (a_1, \ldots, a_i)$. Note: $\mathbf{r} \in \mathcal{R}(i, \ell)$ if and only if $\mathbf{a} \in \mathbb{I}(i, \ell)$ Then we have

$$\begin{aligned}
\sum_{\substack{\mathbf{r} \in \mathcal{R}(i,\ell) \\ \mathbf{s} \in \mathbb{I}(i,m-\ell)}} \prod_{j=1}^{i} q^{\ell-r_j+s_j-1} &= \sum_{\substack{\mathbf{a} \in \mathbb{I}(i,\ell) \\ \mathbf{s} \in \mathbb{I}(i,m-\ell)}} \prod_{j=1}^{i} q^{a_j+s_j-2} \\
&= \left(\sum_{\mathbf{a} \in \mathbb{I}(i,\ell)} q^{\sum_{j=1}^{i}(a_j-1)} \right) \left(\sum_{\mathbf{s} \in \mathbb{I}(i,m-\ell)} q^{\sum_{j=1}^{i}(s_j-1)} \right) \\
&= \left(\sum_{\mathbf{a} \in \mathbb{I}(i,\ell)} q^{\binom{i}{2}} \cdot q^{\delta(\mathbf{a})} \right) \left(\sum_{\mathbf{s} \in \mathbb{I}(i,m-\ell)} q^{\binom{i}{2}} \cdot q^{\delta(\mathbf{s})} \right) \\
&= q^{i^2-i} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q.
\end{aligned}$$

Here we used equation (4) in the final equality. The lemma now follows. □

Let i be a positive integer satisfying $1 \leq i \leq \ell$. Given $P, Q \in G_{\ell,m}$, we say that a sequence $L_1, \ldots, L_i$ of distinct lines connects P to Q if $P \in L_1$, $Q \in L_i$ and for all $1 \leq j < i$, the intersection $L_j \cap L_{j+1}$ is not empty. Then two points P and Q of the Grassmannian are at distance i if and only if there exists a sequence of i lines $L_1, \ldots, L_i$ on the Grassmannian connecting P to Q and no sequence consisting of fewer than i lines connecting P to Q exists. This reformulation of the distance between P and Q is used in [5, Prop. 6.6.2] when discussing Grassmann graphs. We conclude this section by stating the following result from [3, Thm. 24] that indicates the key role of lines on Grassmannians in understanding parity checks and hence decoding of $C(\ell, m)$.

Theorem 2.7. *The minimum distance of the dual Grassmann code $C(\ell, m)^{\perp}$ is three. Further, the three points of $G_{\ell,m}$ corresponding to the support of a minimum weight codeword of $C(\ell, m)^{\perp}$, lie on a line in the Grassmannian. Conversely, any three points on a line in $G_{\ell,m}$, form the support of some minimum weight codeword in $C(\ell, m)^{\perp}$.*

3. Geometry of lines on Grassmannians

In this section we will study the geometry of the lines introduced in the previous section more closely. For the rest of the article, unless it is said specifically, we fix i as a positive integer satisfying $1 \leq i \leq \ell$. The notion of distance motivates the following:

Definition 3.1. Let $P \in G_{\ell,m}$ be a point and let i be an integer satisfying $0 \leq i \leq \ell$. The ith closure $\overline{P}^{(i)}$ of P in $G_{\ell,m}$ is defined by

$$\overline{P}^{(i)} := \{Q \in G_{\ell,m} : \mathrm{dist}(P, Q) \leq i\}.$$

One can think of $\overline{P}^{(i)}$ as a ball of radius i and center P within $G_{\ell,m}$. Alternatively, one can define

$$\begin{aligned} \overline{P}^{(i)} &= \{Q \in G_{\ell,m} : \dim(P \cap Q) \geq \ell - i\} \\ &= \{Q \in G_{\ell,m} : \dim(P + Q) \leq \ell + i\} : \end{aligned}$$

We extend the definition of $\overline{P}^{(i)}$ by setting $\overline{P}^{(i)} = \emptyset$ for any negative integer i and $\overline{P}^{(i)} = G_{\ell,m}$ for $i \geq \ell + 1$. Note that $\overline{P}^{(0)} = \{P\}$ and $\overline{P}^{(\ell)} = G_{\ell,m}$. Geometrically, $\overline{P}^{(i)}$ is the collection of all points Q of the Grassmannian connected to P by a sequence of at most i lines on the Grassmannian.

Remark 3.2. Let i be an integer satisfying $0 \leq i \leq \ell$. Without going into any details, we would like to mention here that the ith closure $\overline{P}^{(i)}$ of P in the Grassmannian $G_{\ell,m}$ is the Schubert variety $\Omega_{\alpha}(\ell, m)$ corresponding to the dimension sequence $\alpha = (i+1, i+2, \ldots, \ell, m-i+1, m-i+2, \ldots, m)$

Note that for every $0 \leq i \leq \ell$ we have $\overline{P}^{(i-1)} \subset \overline{P}^{(i)}$ and that the Grassmannian $G_{\ell,m}$ is the disjoint union of sets $\overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$. More precisely,

$$G_{\ell,m} = \bigsqcup_{i=0}^{\ell} \left(\overline{P}^{(i)} \setminus \overline{P}^{(i-1)}\right). \tag{5}$$

Using Lemma 2.5, one immediately obtains the following:

$$|\overline{P}^{(i)} \setminus \overline{P}^{(i-1)}| = q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q. \tag{6}$$

One can think of the points on $G_{\ell,m}$ as the vertices of the Grassmann graph. Since in a connected graph, one has the notion of a geodesic, this point of view will give rise to geodesics between two points in $G_{\ell,m}$. For a more detailed exposition of geodesics we refer to [5, Sec 1.6] and [25, Sec 1.1.1].

Definition 3.3. Let i be an integer satisfying $0 \leq i \leq \ell$ and let $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ be a point. A geodesic from P to Q is sequence $\mathcal{P} = (Q_0 = P, Q_1, \ldots, Q_{i-1}, Q_i = Q)$ of $i+1$ points in $G_{\ell,m}$ satisfying

$$\mathrm{dist}(P, Q_t) = t, \ \mathrm{dist}(Q_t, Q_{t+1}) = 1, \ \text{and } \mathrm{dist}(Q_t, Q) = i - t, \ \forall\, 1 \leq t \leq i-1.$$

Remark 3.4. It is not hard to see that for every $1 \leq i \leq \ell$ and $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$, a geodesic from P to Q exists. One can construct such a geodesic using induction. For example, let U_1 be a hyperplane of P containing $P \cap Q$. Now take $y \in Q \setminus P \cap Q$ and define $Q_1 = U_1 + \langle y \rangle$. Clearly $P \cap Q_1 = U_1$ and $Q_1 \cap Q = (P \cap Q) + \langle y \rangle$. In other words, $\mathrm{dist}(P, Q_1) = 1$ and $\mathrm{dist}(Q_1, Q) = i - 1$. In the same way we can construct Q_2 by replacing Q with Q_1.

Note that this definition is equivalent with saying that there are i lines $L(U_t, W_t)$ for $1 \leq t \leq i$ connecting P to Q. In this case Q_t is the intersecting point of lines $L(U_t, W_t)$ and $L(U_{t+1}, W_{t+1})$ for every $1 \leq t \leq i-1$. The next lemma is important for the last section of this article and we will be referring to this again and again. This lemma is very similar to [22, Lemma 2.12] and can be deduced immediately from it. For the sake of completeness we include a short proof.

Lemma 3.5. *Let i be an integer satisfying $0 \leq i \leq \ell$, let $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ be a point, and let $\mathcal{P} = (P, Q_1, \ldots, Q_{i-1}, Q)$ be a geodesic from P to Q. Then*

$$P \cap Q_{t+1} \subset P \cap Q_t \ \textit{and}\ P + Q_t \subset P + Q_{t+1} \quad \forall\, 1 \leq t \leq i-1.$$

In particular, $P \cap Q \subset Q_t \subset P + Q$ for every $1 \leq t \leq i-1$.

Proof. Let $1 \leq t \leq i-1$ be arbitrary. We claim that $P \cap Q_{t+1} \subset P \cap Q_t$. If this is not true, then as $\dim(P \cap Q_{t+1}) = \ell - t - 1$, we get $\dim(P \cap Q_t \cap Q_{t+1}) \leq \ell - t - 2$.

Hence,

$$\begin{aligned}\dim((P\cap Q_t)+Q_{t+1}) &= \dim(P\cap Q_t)+\dim(Q_t)-\dim(P\cap Q_t\cap Q_{t+1})\\ &\geq (\ell-t)+\ell-(\ell-t-2)\\ &= \ell+2.\end{aligned}$$

On the other hand, $(P\cap Q_t)+Q_{t+1}\subseteq Q_t+Q_{t+1}$ and $\dim(Q_t+Q_{t+1})=\ell+1$. This is a contradiction and hence we get $P\cap Q_{t+1}\subset P\cap Q_t$.

Similarly, if $P+Q_t\subset P+Q_{t+1}$ is not true then, as $\dim(P+Q_{t+1})=\ell+t+1$, we get $\dim(P+Q_{t+1}+Q_t)\geq \ell+t+1+1=\ell+t+2$. On the other hand, we have $(P+Q_t)\cap Q_{t+1}\supseteq (P\cap Q_{t+1})+(Q_t\cap Q_{t+1})$. Now as $\dim(Q_t\cap Q_{t+1})=\ell-1$, we get $\dim((P+Q_t)\cap Q_{t+1})\geq \ell-1$. Since Q_t is a point from the geodesic, by definition we have $\dim(P+Q_t)=\ell+t$. This gives

$$\begin{aligned}\dim((P+Q_t)+Q_{t+1}) &= \dim(P+Q_t)+\dim Q_{t+1}-\dim((P+Q_t)\cap Q_{t+1})\\ &\leq (\ell+t)+\ell-(\ell-1)\\ &= \ell+t+1,\end{aligned}$$

which is a contradiction. □

For the rest of the article we fix a point $P\in G_{\ell,m}$, an integer $1\leq i\leq \ell$ and a complete flag passing through P:

$$(0)=\mathcal{U}_0\subset\mathcal{U}_1\subset\mathcal{U}_2\subset\cdots\mathcal{U}_{\ell-1}\subset\mathcal{U}_\ell=P=\mathcal{W}_\ell\subset\mathcal{W}_{\ell+1}\subset\cdots\mathcal{W}_{m-1}\subset\mathcal{W}_m=V.$$

We will now investigate geodesics satisfying certain conditions with respect to this flag.

Definition 3.6. Let i be an integer satisfying $0\leq i\leq \ell$ and let $Q\in\overline{P}^{(i)}\setminus\overline{P}^{(i-1)}$ be a point. Given a geodesic $\mathcal{P}$ from P to Q, say $\mathcal{P}=(P,Q_1,\ldots,Q_{i-1},Q)$, we define two i-tuples $\mathbf{r}(\mathcal{P})=(r_1(\mathcal{P}),\ldots,r_i(\mathcal{P}))$ and $\mathbf{s}(\mathcal{P})=(s_1(\mathcal{P}),\ldots,s_i(\mathcal{P}))$, where for $1\leq t\leq i$:

$$r_t(\mathcal{P})=\max\{j:\mathcal{U}_{j-1}\subseteq Q_t\}$$

and

$$s_t(\mathcal{P})=\min\{j:Q_t\subseteq\mathcal{W}_{\ell+j}\}.$$

To ease the notation, we will sometimes write r_t and s_t instead of $r_t(\mathcal{P})$ and $s_t(\mathcal{P})$ if the geodesic $\mathcal{P}$ is fixed. In the next lemma we will show that these i-tuples for a given geodesic from P to a point Q are increasing. More precisely,

Lemma 3.7. *Let i be an integer satisfying $0\leq i\leq\ell$, let $Q\in\overline{P}^{(i)}\setminus\overline{P}^{(i-1)}$, and let a geodesic $\mathcal{P}=(P,Q_1,\ldots,Q_{i-1},Q)$ from P to Q in $G_{\ell,m}$ be given. Then the corresponding i-tuples $\mathbf{r}(\mathcal{P})$ and $\mathbf{s}(\mathcal{P})$ satisfy*

$$\ell\geq r_1\geq r_2\geq\cdots\geq r_i\geq 1 \text{ and } 1\leq s_1\leq\cdots\leq s_i\leq m-\ell.$$

Proof. We only prove the first part involving $\mathbf{r}(\mathcal{P})$. The second part can be shown similarly. Clearly $\ell \geq r_1$. Now let $2 \leq t \leq i$ and let $r_t = j$. By definition, this means $\mathcal{U}_{j-1} \subseteq Q_t$ but $\mathcal{U}_j \nsubseteq Q_t$. As $\mathcal{U}_{j-1} \subset P$, we get $\mathcal{U}_{j-1} \subseteq Q_t \cap P$. From Lemma 3.5 we have $P \cap Q_t \subseteq P \cap Q_{t-1}$. Consequently, $\mathcal{U}_{j-1} \subseteq Q_{t-1}$ and hence $r_{t-1} \geq j$. This completes the proof for the sequence $\mathbf{r}(\mathcal{P})$. □

For any point $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ we define some new constants that are going to be very useful in understanding the geodesics between P and Q.

Definition 3.8. Let i be an integer satisfying $0 \leq i \leq \ell$ and let $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ be a given point. For every $1 \leq t \leq i$ we define

$$\gamma_t(Q) = \max\{j : \dim(Q + \mathcal{U}_j) = \ell + i - t\}$$

and

$$\delta_t(Q) = \min\{j : \dim(Q \cap \mathcal{W}_{\ell+j}) = \ell - i + t\}$$

If from the context the point Q is clear, we will simply write γ_t and δ_t. The constants γ_t indicate the jump positions (in reverse order) in the dimension in the sequence of nested subspaces $Q + \mathcal{U}_0 \subseteq Q + \mathcal{U}_1 \subseteq \cdots \subseteq Q + \mathcal{U}_\ell = Q + P$. Hence $0 \leq \gamma_i < \gamma_{i-1} < \cdots < \gamma_1$. Moreover $\gamma_1 \leq \ell - 1$, since $\dim(P + Q) = \ell + i$. Similarly, the constants δ_t indicate the jump positions in dimension in the sequence of nested subspaces $Q \cap P = Q \cap \mathcal{W}_\ell \subseteq Q \cap \mathcal{W}_{\ell+1} \subseteq \cdots \subseteq Q \cap \mathcal{W}_m = Q$. Hence $1 \leq \delta_1 < \delta_2 < \cdots < \delta_i \leq m - \ell$. In the next theorem, we will show that for every $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ there exists a geodesic such that the corresponding i-tuples are strictly increasing. The constants γ_t and δ_t will appear in a natural way. First we need a lemma.

Lemma 3.9. *Let i be an integer satisfying $0 \leq i \leq \ell$ and let $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$, and recursively define*

$$Q_t := \begin{cases} P & \text{if } t = 0, \\ ((Q_{t-1} \cap Q) + \mathcal{U}_{\gamma_t}) + (\mathcal{W}_{\ell+\delta_t} \cap Q) & \text{if } 1 \leq t \leq i. \end{cases}.$$

Then $\mathcal{P} = (Q_0, \ldots, Q_i)$ is a geodesic from P to Q.

Proof. Directly from the definition, we see that $Q_0 = P$. Moreover, note that $\dim(Q + \mathcal{U}_{\gamma_i}) = \ell$ and $\dim(\mathcal{W}_{\ell+\delta_i} \cap Q) = \ell$. Hence $Q + \mathcal{U}_{\gamma_i} = Q = \mathcal{W}_{\ell+\delta_i} \cap Q$, which implies that $Q_i = Q$.

We will now prove with induction on t the claim that for all $0 \leq t \leq i - 1$:

$$\dim(Q_t) = \ell, \ \dim(P \cap Q_t) = \ell - t, \ \dim(Q_t \cap Q_{t+1}) = \ell - 1, \ \text{and} \ \dim(Q_t \cap Q) = \ell - i + t.$$

If $t = 0$, the only nontrivial statement is that $\dim(P \cap Q_1) = \ell - 1$. We have $Q_1 = ((P \cap Q) + \mathcal{U}_{\gamma_1}) + (\mathcal{W}_{\ell+\delta_1} \cap Q)$. Since $(P \cap Q) + \mathcal{U}_{\gamma_1} \subset P$, we have

$$P \cap Q_1 = ((P \cap Q) + \mathcal{U}_{\gamma_1}) + (P \cap \mathcal{W}_{\ell+\delta_1} \cap Q) = ((P \cap Q) + \mathcal{U}_{\gamma_1}) + (P \cap Q) = (P \cap Q) + \mathcal{U}_{\gamma_1}.$$

Moreover, $\dim((P\cap Q)+\mathcal{U}_{\gamma_1}) = \dim(P\cap Q)+\dim(\mathcal{U}_{\gamma_1})-\dim(P\cap Q\cap\mathcal{U}_{\gamma_1})$. Since $P\cap Q\cap\mathcal{U}_{\gamma_1} = Q\cap\mathcal{U}_{\gamma_1}$ and by definition $\dim(Q+\mathcal{U}_{\gamma_1}) = \ell+i-1$, we may conclude that $\dim(P\cap Q_1) = \ell-1$. Here we computed the dimension $Q\cap\mathcal{U}_{\gamma_1}$ using that $\dim(Q+\mathcal{U}_{\gamma_1}) = \ell+i-1$ by the definition of γ_1.

Now assume that the claim holds for $t-1$. Since $\gamma_t < \gamma_{t-1}$, we get $Q\cap\mathcal{U}_{\gamma_t} \subseteq \mathcal{U}_{\gamma_t} \subset \mathcal{U}_{\gamma_{t-1}}$. The definition of Q_{t-1}, implies $\mathcal{U}_{\gamma_{t-1}} \subset Q_{t-1}$. We conclude $Q\cap\mathcal{U}_{\gamma_t} \subset \mathcal{U}_{\gamma_{t-1}} \subset Q_{t-1}$. Hence inductively we get

$$\begin{aligned}
\dim((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t}) &= \dim(Q_{t-1}\cap Q)+\dim\mathcal{U}_{\gamma_t}-\dim((Q_{t-1}\cap Q)\cap\mathcal{U}_{\gamma_t}) \\
&= (\ell-i+t-1)+\gamma_t-\dim(Q\cap\mathcal{U}_{\gamma_t}) \\
&= (\ell-i+t-1)+\gamma_t-(\gamma_t-i+t) \qquad (7)\\
&= \ell-1.
\end{aligned}$$

By definition of Q_{t-1} we have $\mathcal{W}_{\ell+\delta_{t-1}}\cap Q \subset Q_{t-1}\cap Q$ and using the induction hypothesis, both are of dimension $\ell-i+t-1$. Therefore $\mathcal{W}_{\ell+\delta_{t-1}}\cap Q = Q_{t-1}\cap Q$. As $\delta_t > \delta_{t-1}$, we get $\mathcal{W}_{\ell-\delta_{t-1}} \subset \mathcal{W}_{\ell-\delta_t}$ and hence

$$(Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t} \subset (\mathcal{W}_{\ell+\delta_{t-1}}\cap Q)+\mathcal{U}_{\gamma_t} \subset \mathcal{W}_{\ell+\delta_t}. \qquad (8)$$

Consequently

$$((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t})\cap(\mathcal{W}_{\ell+\delta_t}\cap Q) = ((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t})\cap Q.$$

On the other hand $((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t})\cap Q = (Q_{t-1}\cap Q)+(\mathcal{U}_{\gamma_t}\cap Q)$. But the right-hand side is equal to $Q_{t-1}\cap Q$ as $Q_{t-1} \supseteq \mathcal{U}_{\gamma_{t-1}} \supseteq \mathcal{U}_{\gamma_t}$. Putting all this together, we get

$$\begin{aligned}
\dim Q_t &= (\ell-1)+(\ell-i+t)-\dim((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t})\cap(\mathcal{W}_{\ell+\delta_t}\cap Q) \\
&= (\ell-1)+(\ell-i+t)-\dim(Q_{t-1}\cap Q) \\
&= \ell.
\end{aligned}$$

This proves the first part of the claim that $\dim(Q_t) = \ell$.

The definition of Q_t implies that $((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t})\cap P \subseteq Q_t\cap P$. Now, using the definition of Q_{t-1}, we obtain $P\cap Q_{t-1} \supset P\cap\mathcal{W}_{\ell-\delta_{t-1}}\cap Q = P\cap Q$. Hence, we may conclude that $((Q_{t-1}\cap Q)+\mathcal{U}_{\gamma_t})\cap P = (P\cap Q)+\mathcal{U}_{\gamma_t}$. Moreover, $\dim((P\cap Q)+\mathcal{U}_{\gamma_t}) = \ell-t$, since $\dim(Q+\mathcal{U}_{\gamma_t}) = \ell-i+t$. Combining the above, we get $\dim(P\cap Q_t) \geq \ell-t$ and consequently $\mathrm{dist}(P,Q_t) \leq t$. Similarly, as $\mathcal{W}_{\ell+\delta_t}\cap Q \subset Q_t\cap Q$, one obtains $\dim(Q_t\cap Q) \geq \ell-i+t$ and hence $\mathrm{dist}(Q,Q_t) \leq i-t$. As $\mathrm{dist}(P,Q) = i$ we conclude $\mathrm{dist}(P,Q_t) = t$ and $\mathrm{dist}(Q,Q_t) = i-t$. This proves that $\dim(P\cap Q_t) = \ell-t$ and $\dim(Q\cap Q_t) = \ell-i+t$.

What remains to be shown is that $\dim(Q_t\cap Q_{t+1}) = \ell-1$. Since $(Q\cap Q_t)+\mathcal{U}_{\gamma_{t+1}} \subset Q_t$, we obtain that

$$Q_t\cap Q_{t+1} = ((Q\cap Q_t)+\mathcal{U}_{\gamma_{t+1}})+(\mathcal{W}_{\ell+\delta_{t+1}}\cap Q\cap Q_t) = (Q\cap Q_t)+\mathcal{U}_{\gamma_{t+1}}.$$

Similarly as in equation (7), we can now show that $\dim(Q_t \cap Q_{t+1}) = \ell - 1$. This proves the claim.

The claim immediately implies that $\mathcal{P}$ is a geodesic from P to Q. □

Theorem 3.10. *Let i be an integer satisfying $0 \leq i \leq \ell$. For every $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$, the i-tuples $\mathbf{r}(\mathcal{P})$ and $\mathbf{s}(\mathcal{P})$ corresponding to the geodesic $\mathcal{P}$ constructed in Lemma 3.9, are given by*

$$r_t = \gamma_t(Q) + 1 \text{ and } s_t = \delta_t(Q), \text{ for } 1 \leq t \leq i.$$

In particular these i-tuples satisfy:

$$\ell \geq r_1 > r_2 > \cdots > r_i \geq 1 \text{ and } 1 \leq s_1 < \cdots < s_i \leq m - \ell.$$

Proof. We will use the geodesic $\mathcal{P}$ constructed in Lemma 3.9 and determine its i-tuples $\mathbf{r}(\mathcal{P})$ and $\mathbf{s}(\mathcal{P})$. First, we claim that $r_t = \gamma_t + 1$. Recall that

$$r_t = \max\{j : \mathcal{U}_{j-1} \subseteq Q_t\}.$$

By definition, we have $\mathcal{U}_{\gamma_t} \subset Q_t$. This gives $r_t \geq \gamma_t + 1$. On the other hand if $\mathcal{U}_{\gamma_t+1} \subset Q_t$ then $\mathcal{U}_{\gamma_t+1} + Q \subseteq Q_t + Q$. But we also have $\dim(Q_t + Q) = \ell + i - t$ and by definition of γ_t we get $\dim(\mathcal{U}_{\gamma_t+1} + Q) > \dim(\mathcal{U}_{\gamma_t} + Q) = \ell + i - t$. But this is a contradiction. This implies $\mathcal{U}_{\gamma_t+1} \nsubseteq Q_t$. In particular, $r_t \leq \gamma_t + 1$ and hence $r_t = \gamma_t + 1$ for every $1 \leq t \leq i$. Also, recall that

$$s_t = \min\{j : Q_t \subset W_{\ell+j}\}.$$

Using equation (8), we know $Q_t \subset \mathcal{W}_{\ell+\delta_t}$ and hence $s_t \leq \delta_t$. Now, if $Q_t \subseteq \mathcal{W}_{\ell+\delta_t-1}$ then $Q_t \cap Q \subseteq \mathcal{W}_{\ell+\delta_t-1} \cap Q$. Note that this gives $\dim(\mathcal{W}_{\ell+\delta_t-1} \cap Q) \geq \ell - i + t$ but by definition of δ_t we have $\dim(\mathcal{W}_{\ell+\delta_t-1} \cap Q) < \ell - i + t$. This is a contradiction. Hence we get $s_t = \delta_t$ for every $1 \leq t \leq i$. This completes the proof of the theorem. □

Remark 3.11. Note that the geodesic $\mathcal{P}$ constructed in Lemma 3.9 only depends on P, Q and the flag. Since P and the flag are fixed throughout, we will therefore for this geodesic use the notations $\mathbf{r}(Q)$ and $\mathbf{s}(Q)$ instead of $\mathbf{r}(\mathcal{P})$ and $\mathbf{s}(\mathcal{P})$.

In the next theorem we will prove that for a given $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ there is a unique geodesic $(P, Q_1, \ldots, Q_{i-1}, Q)$ such that the corresponding i-tuples $\mathbf{r} = (r_1, \ldots, r_i)$ and $\mathbf{s} = (s_1, \ldots, s_i)$ satisfy the strict inequality condition. This implies in particular that this geodesic has to be the one constructed in Lemma 3.9.

Theorem 3.12. *Let i be an integer satisfying $0 \leq i \leq \ell$ and let $Q \in \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$ and let $\mathcal{P}' = (P, Q'_1, \ldots, Q'_{i-1}, Q)$ be an arbitrary geodesic from P to Q. Let $\mathbf{r}(\mathcal{P}') = (r'_1, \ldots, r'_i)$ and $\mathbf{s}'(\mathcal{P}') = (s'_1, \ldots, s'_i)$ are corresponding i-tuples and suppose that*

$$r'_1 > \cdots > r'_i \text{ and } s'_1 < \cdots < s'_i.$$

Then $Q'_j = Q_j$ for every $1 \leq j \leq i$, where the Q_j are defined as in Lemma 3.9.

Proof. We claim that $r'_t = \gamma_t + 1$ for every $1 \leq t \leq i$. Since $\mathcal{U}_{r'_t-1} \subset Q'_t$, we get $\mathcal{U}_{r'_t-1} + Q \subset Q'_t + Q$ and hence $\dim(\mathcal{U}_{r'_t-1} + Q) \leq \dim(Q'_t + Q) = \ell + i - t$. By definition of γ_t we get $r'_t - 1 \leq \gamma_t$. Now, if $r'_t - 1 < \gamma_t$, then we get $\dim(\mathcal{U}_{r'_t} + Q) = \dim(\mathcal{U}_{r'_k-1} + Q)$ for some $k > t$. As $\mathcal{U}_{r'_k-1} \subset \mathcal{U}_{r'_t-1}$, we obtain that $\mathcal{U}_{r'_t-1} + Q = \mathcal{U}_{r'_k-1} + Q$. Intersecting both sides of this equality with P, we get $\mathcal{U}_{r'_t-1} + (Q \cap P) = \mathcal{U}_{r'_k-1} + (Q \cap P)$. By Lemma 3.5, we have $P \cap Q \subset Q'_k$ and moreover $\mathcal{U}_{r'_k-1} \subset Q'_k$ by definition of r'_k. Hence $\mathcal{U}_{r'_t-1} \subset \mathcal{U}_{r'_t-1} + (Q \cap P) = \mathcal{U}_{r'_k-1} + (Q \cap P) \subseteq Q'_k$, implying $r'_k \geq r'_t$. But this contradicts the strict inequality $r'_k < r'_t$. Therefore, we get $r'_t - 1 = \gamma_t$.

Similarly, from the definition of s'_t we have $Q'_t \subseteq \mathcal{W}_{\ell+s'_t}$ and this gives $\dim(\mathcal{W}_{\ell+s'_t} \cap Q) \geq \dim(Q'_t \cap Q) = \ell - i + t$. Consequently, $\delta_t \leq s'_t$. Now if $\delta_t < s'_t$, then $\dim(\mathcal{W}_{\ell+s'_t} \cap Q) = \dim(\mathcal{W}_{\ell+s'_k} \cap Q)$ for some $k > t$. Then $\mathcal{W}_{\ell+s'_t} \cap Q = \mathcal{W}_{\ell+s'_k} \cap Q$. Adding P both sides and keeping in mind that $P \subset \mathcal{W}_{\ell+j}$ for every j, we get $\mathcal{W}_{\ell+s'_t} \cap (P + Q) = \mathcal{W}_{\ell+s'_k} \cap (P + Q)$. Since $Q'_k \subset \mathcal{W}_{\ell+s'_k}$ by definition of s'_k and $Q'_k \subset P + Q$ by Lemma 3.5, we get $Q'_k \subset \mathcal{W}_{\ell+s'_j}$ and consequently, $s'_k \leq s'_t$. But this contradicts the strict inequality $s'_k > s'_t$. Hence $s'_t = \delta_t$.

Now, we will show that $Q_t = Q'_t$ for $1 \leq t \leq i$ by induction on t. It is enough to prove that for every $1 \leq t \leq i$, $(Q_{t-1} \cap Q) + \mathcal{U}_{\gamma_t} \subseteq Q'_t$ and $\mathcal{W}_{\ell+\delta_t} \cap Q \subseteq Q'_t$.

If $t = 1$, then $(Q_{t-1} \cap Q) + \mathcal{U}_{\gamma_t} = (P \cap Q) + \mathcal{U}_{\gamma_1}$, which is contained in Q'_1, since $P \cap Q \subset Q'_1$ by Lemma 3.5 and $\mathcal{U}_{\gamma_1} \subset Q'_1$ by definition of r'_1 and the fact that $r'_1 - 1 = \gamma_1$. Similarly by definition of s'_1 and the fact that $s'_1 = \delta_1$, we get $\mathcal{W}_{\ell+\delta_1} \cap Q \supseteq Q'_1 \cap Q$. Since both spaces have dimension $\ell - i + 1$, they are equal. Hence $\mathcal{W}_{\ell+\delta_1} \cap Q \subseteq Q'_1$.

Now for the induction step assume $t > 1$ and $Q_j = Q'_j$ for every $1 \leq j \leq t - 1$. We have $(Q_{t-1} \cap Q) + \mathcal{U}_{\gamma_t} = (Q'_{t-1} \cap Q) + \mathcal{U}_{\gamma_t}$. Applying Lemma 3.5 to the geodesic $(Q'_{t-1}, \ldots, Q'_{i-1}, Q)$, we see that $Q'_{t-1} \cap Q \subset Q'_t$. Moreover, since $r'_t - 1 = \gamma_t$, we get $\mathcal{U}_{\gamma_t} \subset Q'_t$. This shows that $(Q_{t-1} \cap Q) + \mathcal{U}_{\gamma_t} \subset Q'_t$. Similarly as in the induction basis, by definition of s'_t and the fact that $s'_t = \delta_t$, we get $\mathcal{W}_{\ell+\delta_t} \cap Q \supseteq Q'_t \cap Q$. Since both spaces have dimension $\ell - i + t$, they are equal. Hence $\mathcal{W}_{\ell+\delta_t} \cap Q \subseteq Q'_t$. This concludes the proof. □

4. A majority logic decoder for $C(\ell, m)$

Our aim in this section is to construct a decoder for the Grassmann codes $C(\ell, m)$ that runs in quadratic complexity in the length of the code. In order to do this, we will construct certain "orthogonal" parity checks of $C(\ell, m)$ and then use the well-known method of majority logic decoding. First, we recall what we mean by orthogonal parity checks and how to use them for majority logic decoding. For a general reference on these topics, see [16, Ch 13.7] for the binary case and [18, Ch 1] for the q-ary case. As usual, we call a codeword of the dual code $C(\ell, m)^\perp$ a parity check for $C(\ell, m)$.

Definition 4.1. Let C be an $[n, k]$ code. For $1 \leq i \leq n$, a set $\mathcal{J}$ of J parity checks of C is said to be orthogonal on the ith coordinate if the $J \times n$ matrix H having these J parity checks as rows satisfies the following:

(1) Each entry in the ith column of H is 1.
(2) The Hamming weight of any other column of H is at most 1, i.e., if $j \neq i$ and the jth column of H contains a non-zero entry in the rth row, then this is the only non-zero entry in this column.

Suppose that $c \in C$ is the sent codeword, but that the receiver receives the word $w = c + e$, for some $e = (e_1, \ldots, e_n) \in \mathbb{F}_q^n$. Given a coordinate i and a set $\mathcal{J} = \{\omega_1, \ldots, \omega_J\}$ of parity checks orthogonal on the ith coordinate, we define $S_j(w) := \sum_{a=1}^{n} w_a \omega_{j,a}$. Note that $S_j(w) = S_j(e) = e_i + \sum_{a=1; a\neq i}^{n} e_a \omega_{j,a}$. Now if a clear majority of the J values $S_j(w) - w_i$, where $1 \leq j \leq J$, equals $-\alpha$, then we define $\widehat{c}_i := \alpha$. In case of a tie, we set $\widehat{c}_i := w_i$. Doing this for each coordinate i, results in the decoded word $\widehat{c} := (\widehat{c}_1, \ldots, \widehat{c}_n)$. This procedure of determining $\widehat{c}$ is called majority logic decoding. It is not a priori clear that $\widehat{c}$ is a codeword or if it is, then it is equal to the sent codeword c. However, the following theorem from [18] guarantees that $\widehat{c} = c$ as long as the number of errors, i.e., the Hamming weight of e is at most $\lfloor J/2 \rfloor$. For ease of reference, we include a proof, based on the proof given in [18, Ch 1,Thm 1].

Theorem 4.2. [18, Ch. 1,Thm. 1] *Let C be an $[n, k]$ code such that for each $1 \leq i \leq n$, there exists a set $\mathcal{J}$ of J orthogonal parity checks on the ith coordinate. Then the corresponding majority logic decoder corrects up to $\lfloor J/2 \rfloor$ errors.*

Proof. Let c be a transmitted codeword and $w = c + e$ be the received word with error $e \in \mathbb{F}_q^n$. Assume that no more than $\lfloor J/2 \rfloor$ errors have occurred. It is enough to prove that if we have a set $\mathcal{J} = \{\omega_1, \ldots, \omega_J\}$ of J parity checks of C orthogonal on the ith coordinate, then we can determine the value of e_i by majority voting. As before, we have,

$$S_j(w) = S_j(e) = e_i + \sum_{a\neq i}^{n} e_a \omega_{j,a}, \text{ for } 1 \leq j \leq J.$$

Now we distinguish two cases.

If $e_i \neq 0$, then e_i is an error position. Since there are not more than $\lfloor J/2 \rfloor$ errors and the set $\mathcal{J}$ is orthogonal on the ith coordinate, the remaining $\lfloor J/2 \rfloor - 1$ errors can appear in at most $\lfloor J/2 \rfloor - 1$ equations above. As a result, at least $J - \lfloor J/2 \rfloor + 1$ expressions $S_j(w)$ have the value e_i, i.e., the majority of $S_j(w)$ assumes the value e_i.

On the other hand, if $e_i = 0$, for $1 \leq j \leq J$, we have

$$S_j(w) = S_j(e) = \sum_{t\neq i}^{n} e_t \omega_{j,t}.$$

Among these expressions, at most $\lfloor J/2 \rfloor$ can involve some error positions. Hence at least $J - \lfloor J/2 \rfloor$ expressions $S_j(w)$ are zero. In other words, at least half of the expressions $S_j(w)$ have the same value as e_i.

Thus, in either case, majority logic decoding recovers the i-th coordinate of the sent codeword. □

To use this theorem for the decoding of Grassmann codes, we need to construct as many orthogonal parity checks as possible for each coordinate. However, as the automorphism group of $C(\ell, m)$ acts transitively on the coordinates, we only need to produce such parity checks for a single fixed coordinate. Then sets of parity checks orthogonal on other coordinates can be obtained immediately. Therefore, for the rest of the article we fix $P \in G_{\ell,m}$ and will construct parity checks that are orthogonal on the coordinate corresponding to P. The starting point of our construction is Theorem 2.7. First, note that if we take a line in $G_{\ell,m}$ passing through P and any two points Q and R different from P on that line, then Theorem 2.7 guarantees the existence of a parity check for $C(\ell, m)$ with support corresponding to P, Q and R. Note that if $q = 2$, for a given line through P, there is a unique choice for Q and R, since in that case a line contains exactly three points. In this way, we can obtain for each line one parity check of Hamming weight 3 whose support contains P. All the parity checks obtained in this way are orthogonal on P as they all are passing through P and any two distinct lines through P only intersect at P. In this way we get $\begin{bmatrix} \ell \\ 1 \end{bmatrix}_q \begin{bmatrix} m-\ell \\ 1 \end{bmatrix}_q$ many parity checks orthogonal on P. Before giving the general construction, we illustrate in the next example how are we are going to use the parity checks corresponding to lines through P to increase the set of parity checks orthogonal on P.

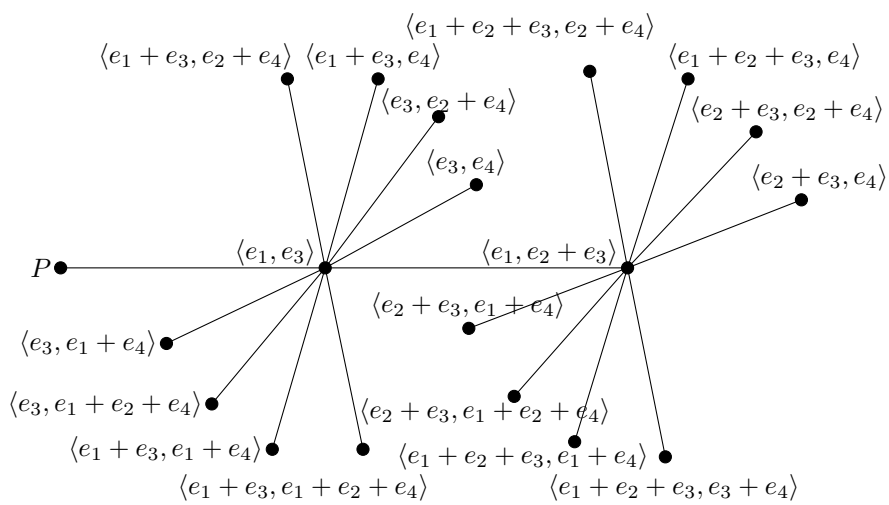
Example 4.3. Let $V = \mathbb{F}_2^4$ and let $G_{2,4}$ be the Grassmannian of all planes of V. Let $C(2, 4)$ be the corresponding binary Grassmann code. Then $C(2, 4)$ is a binary $[n, k, d]$ code where

$$n = \begin{bmatrix} 4 \\ 2 \end{bmatrix}_2 = 35, \quad k = 6, \quad \text{and} \quad d = 16.$$

Now let $\{e_1, \ldots, e_4\}$ be the standard basis of V and $P = \langle e_1, e_2 \rangle$. There are $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_2 \begin{bmatrix} 2 \\ 1 \end{bmatrix}_2 = 9$ lines in $G_{2,4}$ passing through P. Explicitly these lines are $L(U, W)$, where there are three possible choices for U, namely $\langle e_1 \rangle$, $\langle e_2 \rangle$, or $\langle e_1 + e_2 \rangle$, and three possibilities for W, namely $\langle e_1, e_2, e_3 \rangle$, $\langle e_1, e_2, e_4 \rangle$, or $\langle e_1, e_2, e_3 + e_4 \rangle$. For example, we have $L(\langle e_1 \rangle, \langle e_1, e_2, e_3 \rangle) = \{P, \langle e_1, e_3 \rangle, \langle e_1, e_2 + e_3 \rangle\}$.

Each of these nine lines corresponds to a weight three parity check. These parity checks are orthogonal on P. As mentioned before, the three points on these lines form the support of the corresponding parity check. To increase the number of parity checks orthogonal on P, we combine the nine we have found so far with other weight three parity checks in a structured way. Consider the line

$L(\langle e_1\rangle, \langle e_1, e_2, e_3\rangle)$. There are nine lines through $\langle e_1, e_3\rangle$. Let $L(U, W)$ be a line through $\langle e_1, e_3\rangle$. One can verify directly that if $U \neq \langle e_1\rangle$ and $W \neq \langle e_1, e_2, e_3\rangle$, then the two points on $L(U, W)$ different from $\langle e_1, e_3\rangle$, lie in $\overline{P}^{(2)} \backslash \overline{P}^{(1)}$. In this way, we get four lines through $\langle e_1, e_3\rangle$ intersecting $\overline{P}^{(1)}$ only at $\langle e_1, e_3\rangle$. Similarly we will get four such lines passing through the third point $\langle e_1, e_2 + e_3\rangle$. The lines are given in the figure below. Now, we enumerate the four lines through $\langle e_1, e_3\rangle$, say $m_1 = L(\langle e_3\rangle, \langle e_1, e_3, e_4\rangle)$, $m_2 = L(\langle e_3\rangle, \langle e_1, e_3, e_2 + e_4\rangle)$, $m_3 = L(\langle e_1 + e_3\rangle, \langle e_1, e_3, e_4\rangle)$, $m_4 = L(\langle e_1 + e_3\rangle, \langle e_1, e_3, e_2 + e_4\rangle)$, as well as the four lines through $\langle e_1, e_2 + e_3\rangle$, say $n_1 = L(\langle e_2 + e_3\rangle, \langle e_1, e_2 + e_3, e_4\rangle)$, $n_2 = L(\langle e_2 + e_3\rangle, \langle e_1, e_2 + e_3, e_2 + e_4\rangle)$, $n_3 = L(\langle e_1 + e_2 + e_3\rangle, \langle e_1, e_2 + e_3, e_4\rangle)$, $n_4 = L(\langle e_1 + e_2 + e_3\rangle, \langle e_1, e_2 + e_3, e_2 + e_4\rangle)$. Let ω be the parity check corresponding to the line $L(\langle e_1\rangle, \langle e_1, e_2, e_3\rangle)$, ω_i be the parity check corresponding to the ith line through $\langle e_1, e_3\rangle$ and ω_i' be the parity check corresponding to the ith line through $\langle e_1, e_2 + e_3\rangle$. For every i the parity check $\omega + \omega_i + \omega_i'$ is of weight five. Further, these four weight five parity checks are again orthogonal on P as their supports consists of P and pairwise disjoint sets of four points from $\overline{P}^{(2)} \setminus \overline{P}$. Therefore the set of $9 + 4 = 13$ parity checks obtained in this way is orthogonal on P. Note that we can not increase the set of these parity checks any further. This is simply because the total support of these 13 parity checks consists of $1 + 9 \times 2 + 4 \times 4 = 35$ points. However, $G_{2,4}$ contains exactly that many points, so there is no room for any further parity checks without violating orthogonality. Now using the automorphism group, we can for each coordinate produce a set of 13 parity checks orthogonal on that coordinate. Theorem 4.2 implies that we can correct up to six errors for $C(2, 4)$ using this approach.



Note that any parity check gives rise to a geodesic from P to a point either in $\overline{P}$ or in $\overline{P}^{(2)}$. For example, the parity check corresponding to the line $L(\langle e_1 + e_2\rangle, \langle e_1, e_2, e_4\rangle)$ gives rise to two geodesics: $(P, \langle e_1 + e_2, e_4\rangle)$ and $(P, \langle e_1 + e_2, e_2 +$

$e_4\rangle)$. The parity check $\omega+\omega_1+\omega_1'$ described above, gives rise to four geodesics $(P,\langle e_1,e_3\rangle,\langle e_3,e_4\rangle)$, $(P,\langle e_1,e_3\rangle,\langle e_3,e_1+e_4\rangle)$, $(P,\langle e_1,e_2+e_3\rangle,\langle e_2+e_3,e_4\rangle)$, and $(P,\langle e_1,e_2+e_3\rangle,\langle e_2+e_3,e_1+e_4\rangle)$. This is the reason we studied geodesics in the previous section. If we fix the flag $0\subset\langle e_1\rangle\subset\langle e_1,e_2\rangle\subset\langle e_1,e_2,e_3\rangle\subset V$, then both the geodesics $(P,\langle e_1+e_2,e_4\rangle)$ and $(P,\langle e_1+e_2,e_2+e_4\rangle)$ have the same 1-tuples, namely $\mathbf{r}=(2)$ and $\mathbf{s}=(1)$. The four geodesics coming from the parity check $\omega+\omega_1+\omega_1'$ have the same 2-tuples, namely $\mathbf{r}=(2,1)$ and $\mathbf{s}=(1,2)$. Note that both $\mathbf{r}$ and $\mathbf{s}$ are strictly monotonic. It is possible to consider other parity checks of weight five, for example one obtained by combining the lines $L(\langle e_1\rangle,\langle e_1,e_2,e_4\rangle)$, $L(\langle e_4\rangle,\langle e_1,e_2,e_4\rangle)$, and $L(\langle e_2+e_4\rangle,\langle e_1,e_3,e_2+e_4\rangle)$. Also this parity check would give rise to four geodesics, one of them being $(P,\langle e_1,e_4\rangle,\langle e_3,e_4\rangle)$. The 2-tuples for these four geodesics are also the same, namely $\mathbf{r}=(2,1)$ and $\mathbf{s}=(2,2)$. Note that the strict monotonicity is not satisfied in $\mathbf{s}$. We see that in this example, we can get a maximal set of parity checks orthogonal on P by studying geodesics starting at P of varying lengths with strict monotonic $\mathbf{r}$ and $\mathbf{s}$ tuples. This is the reason we studied geodesics where both $\mathbf{r}$ and $\mathbf{s}$ are strictly monotonic in Theorems 3.10 and 3.12.

In the next theorem we show that the observations from the previous example can be generalized for any code $C(\ell,m)$. Recall that for $Q\in\overline{P}^{(i)}\setminus\overline{P}^{(i-1)}$, we defined the i-tuples $\mathbf{r}(Q)$ and $\mathbf{s}(Q)$ in Remark 3.11. In view of Theorem 3.12 these are the i-tuples of the unique geodesic from P to Q having strictly monotonic i-tuples. Also recall that, throughout we are working with a fixed complete flag of V, namely

$$(0)=\mathcal{U}_0\subset\mathcal{U}_1\subset\mathcal{U}_2\subset\cdots\mathcal{U}_{\ell-1}\subset\mathcal{U}_\ell=P=\mathcal{W}_\ell\subset\mathcal{W}_{\ell+1}\subset\cdots\mathcal{W}_{m-1}\subset\mathcal{W}_m=V.$$

Theorem 4.4. *Let ℓ,m be positive integers satisfying $\ell\le m$ and $C(\ell,m)$ be the corresponding Grassmann code. Then for every $1\le i\le\ell$ there exists a set $\mathcal{J}_i$ of $J_i:=\left\lfloor\frac{q}{2}\right\rfloor^i q^{i^2-i}\begin{bmatrix}\ell\\ i\end{bmatrix}_q\begin{bmatrix}m-\ell\\ i\end{bmatrix}_q$ many parity checks of $C(\ell,m)$ of Hamming weight $1+2^i$ such that:*

(1) For any $\omega\in\mathcal{J}_i$, the support of ω consists of P and 2^i points from the set $\overline{P}^{(i)}\setminus\overline{P}^{(i-1)}$.

(2) For any $\omega\in\mathcal{J}_i$ and $Q,Q'\in\mathrm{Supp}(\omega)\backslash\{P\}$, we have

$$\mathbf{r}(Q)=\mathbf{r}(Q')\quad\text{and}\quad\mathbf{s}(Q)=\mathbf{s}(Q').$$

(3) For any two distinct $\omega,\omega'\in\mathcal{J}_i$ we have $\mathrm{Supp}(\omega)\cap\mathrm{Supp}(\omega')=\{P\}$.

(4) For any i-tuples $(r_1,\dots,r_i)$ and $(s_1,\dots,s_i)$ satisfying $\ell\ge r_1>\cdots>r_i\ge1$ and $1\le s_1<\cdots<s_i\le m-\ell$, there exist exactly $\left\lfloor\frac{q}{2}\right\rfloor^i\prod_{j=1}^i q^{\ell-r_j+s_j-1}$ parity checks ω in $\mathcal{J}_i$, such that:
for any $Q\in\mathrm{Supp}(\omega)\backslash\{P\}$, $\mathbf{r}(Q)=(r_1,\dots,r_i)$ and $\mathbf{s}(Q)=(s_1,\dots,s_i)$.

Proof. The proof is by induction on i. Assume $i = 1$. For each line, we obtain $\lfloor q/2 \rfloor$ parity checks of weight three as follows. We partition the points on the line distinct from P into $\lfloor q/2 \rfloor$ subsets of cardinality two and, if q is odd, a subset containing only one point. For each such subset, say $\{Q, R\}$ there is a parity check ω such that $\mathrm{Supp}(\omega) = \{P, Q, R\}$, by Theorem 2.7. Since there are $\begin{bmatrix} \ell \\ 1 \end{bmatrix}_q \begin{bmatrix} m-\ell \\ 1 \end{bmatrix}_q$ lines in $G_{\ell,m}$ through P, we obtain a set $\mathcal{J}_1$ with $\lfloor q/2 \rfloor \begin{bmatrix} \ell \\ 1 \end{bmatrix}_q \begin{bmatrix} m-\ell \\ 1 \end{bmatrix}_q$ parity checks. It is clear that these parity checks satisfy items (1) and (3).

We now show that for any two given points Q, Q', not equal to P, on a line $L(U, W)$ through P it holds that $r_1(Q) = r_1(Q')$ and $s_1(Q) = s_1(Q')$. From this item (2) will follow. Since $U = P \cap Q = P \cap Q'$ and $\mathcal{U}_t \subseteq P$ for every $0 \leq t \leq \ell$, we get

$$\begin{aligned} r_1(Q) &= \max\{j : \mathcal{U}_{j-1} \subseteq Q\} \\ &= \max\{j : \mathcal{U}_{j-1} \subseteq P \cap Q\} \\ &= \max\{j : \mathcal{U}_{j-1} \subseteq P \cap Q'\} \\ &= \max\{j : \mathcal{U}_{j-1} \subseteq Q'\} \\ &= r_1(Q'). \end{aligned}$$

Similarly, as $W = P + Q = P + Q'$ and $P \subseteq \mathcal{W}_{\ell+t}$ for every $0 \leq t \leq m - \ell$, we get

$$\begin{aligned} s_1(Q) &= \min\{j : Q \subset \mathcal{W}_{\ell+j}\} \\ &= \min\{j : P + Q \subset \mathcal{W}_{\ell+j}\} \\ &= \min\{j : P + Q' \subset \mathcal{W}_{\ell+j}\} \\ &= \min\{j : Q' \subset \mathcal{W}_{\ell+j}\} \\ &= s_1(Q'). \end{aligned}$$

To complete the induction basis, we show item (4). Let $\ell \geq r_1 \geq 1$ and $1 \leq s_1 \leq m - \ell$ be given. Consider all $(\ell - 1)$-dimensional $U \subset P$ such that $\mathcal{U}_{r_1-1} \subset U$ but $\mathcal{U}_{r_1} \nsubseteq U$. There are exactly $\begin{bmatrix} \ell-r_1+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} \ell-r_1 \\ 1 \end{bmatrix}_q = q^{\ell-r_1}$ such spaces. Similarly, consider all $(\ell + 1)$-dimensional spaces W satisfying $P \subset W \subset \mathcal{W}_{\ell+s_1}$ but $W \nsubseteq \mathcal{W}_{\ell+s_1-1}$. There are exactly $\begin{bmatrix} s_1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} s_1-1 \\ 1 \end{bmatrix}_q = q^{s_1-1}$ such W. Now take any point Q distinct from P on a line $L(U, W)$, with U and W chosen as above. Then by construction $r_1(Q) = r_1$, since $\mathcal{U}_{r_1-1} \subset U \subset Q$, while $\mathcal{U}_{r_1} \subset Q$ would imply that $\mathcal{U}_{r_1} \subset Q \cap P = U$ using that $\mathcal{U}_{r_1} \subset P$. Similarly $s_1(Q) = s_1$. If either U contains $\mathcal{U}_{r_1}$ or W is contained in $\mathcal{W}_{\ell-s_1-1}$, then for any point Q on $L(U, W)$, we have $r_1(Q) > r_1$ or $s_1(Q) < s_1$. Hence no other parity checks in $\mathcal{J}_1$ satisfy the requirements from item (4). This completes the proof of item (4).

Now we consider the induction step. Assume that $i \geq 2$ and that the theorem is true for $i-1$. Let $\mathbf{r} = (r_1, \ldots, r_i)$ and $\mathbf{s} = (s_1, \ldots, s_i)$ be two given i-tuples satisfying $\ell \geq r_1 > \cdots > r_i \geq 1$ and $1 \leq s_1 < \cdots < s_i \leq m - \ell$. Then $\ell \geq r_1 > \cdots > r_{i-1} > 1$ and $1 \leq s_1 < \cdots < s_{i-1} < m - \ell$. By the induction hypothesis, we know that there

exist precisely $\lfloor q/2\rfloor^{i-1}\prod_{j=1}^{i-1} q^{\ell-r_j+s_j-1}$ parity checks ω in $\mathcal{J}_{i-1}$ with $(i-1)$-tuples $(r_1,\ldots,r_{i-1})$ and $(s_1,\ldots,s_{i-1})$. For any of these parity checks, we are going to construct a set $\mathcal{J}_i(\mathbf{r},\mathbf{s})$ consisting of exactly $\lfloor q/2\rfloor q^{\ell-r_i+s_i-1}$ parity checks of weight $1+2^i$ satisfying (1), (2), (3), and having i-tuples $\mathbf{r}$ and $\mathbf{s}$.

Choose $Q_{i-1}\in \mathrm{Supp}(\omega)\setminus\{P\}$, then by Theorems 3.10 and 3.12 there exists a unique geodesic $\mathcal{P}_{i-1}=(P,Q_1,\ldots,Q_{i-1})$ from P to Q_{i-1} such that $\mathbf{r}(\mathcal{P}_{i-1})=(r_1,\ldots,r_{i-1})$ and $\mathbf{s}(\mathcal{P}_{i-1})=(s_1,\ldots,s_{i-1})$. We claim that there exist $q^{\ell-r_i+s_i-1}$ many lines $L(U,W)$ in $G_{\ell,m}$ passing though Q_{i-1} such that for any point Q_i on $L(U,W)$ different from Q_{i-1}, the sequence $\mathcal{P}_i=(P,Q_1,\ldots,Q_{i-1},Q_i)$ is a geodesic from P to Q_i satisfying $\mathbf{r}(\mathcal{P}_i)=(r_1,\ldots,r_i)$ and $\mathbf{s}(\mathcal{P}_i)=(s_1,\ldots,s_i)$. First of all, if $L(U,W)$ is a line through Q_{i-1} such that for one point Q_i on $L(U,W)$ different from Q_{i-1}, the sequence $\mathcal{P}_i=(P,Q_1,\ldots,Q_{i-1},Q_i)$ is a geodesic from P to Q_i satisfying $\mathbf{r}(\mathcal{P}_i)=(r_1,\ldots,r_i)$ and $\mathbf{s}(\mathcal{P}_i)=(s_1,\ldots,s_i)$, then the same is true for all the other points on $L(U,W)$ as well. Indeed, if Q_i' is another point on $L(U,W)$, then somewhat similarly as in the induction basis, one obtains

$$\begin{aligned}
r_i=r_i(Q_i) &= \max\{j:\mathcal{U}_{j-1}\subseteq Q_i\}\\
&= \max\{j:\mathcal{U}_{j-1}\subseteq Q_{i-1}\cap Q_i\} \quad \text{since } \mathcal{U}_{r_i-1}\subseteq \mathcal{U}_{r_{i-1}-1}\subseteq Q_{i-1}\\
&= \max\{j:\mathcal{U}_{j-1}\subseteq Q_{i-1}\cap Q_i'\} \quad \text{since } Q_{i-1}\cap Q_i=U=Q_{i-1}\cap Q_i'\\
&= \max\{j:\mathcal{U}_{j-1}\subseteq Q_i'\} \quad \text{since } \mathcal{U}_{r_i(Q_i')-1}\subseteq \mathcal{U}_{r_{i-1}-1}\subseteq Q_{i-1}\\
&= r_i(Q_i').
\end{aligned}$$

Similarly one obtains $s_i(Q_i')=s_i$.

To obtain the number of possible lines $L(U,W)$ it is now enough to count the number of points Q_i in $G_{\ell,m}$ satisfying:

(a) $\dim(Q_{i-1}\cap Q_i)=\ell-1$,
(b) $\dim(P\cap Q_i)=\ell-i$,
(c) $\mathbf{r}(Q_i)=(r_1,\ldots,r_i)$, i.e $\mathcal{U}_{r_i-1}\subseteq Q_i$ but $\mathcal{U}_{r_i}\nsubseteq Q_i$, and
(d) $\mathbf{s}(Q_i)=(s_1,\ldots,s_i)$, i.e. $Q_i\subseteq \mathcal{W}_{\ell+s_i}$ but $Q_i\nsubseteq \mathcal{W}_{\ell+s_i-1}$.

Indeed, the first two condition are equivalent to saying that $\mathcal{P}_i=(P,Q_1,\ldots,Q_{i-1},Q_i)$ is a geodesic from P to Q_i, while the last two conditions guarantee that $\mathbf{r}(\mathcal{P}_i)=(r_1,\ldots,r_i)$ and $\mathbf{s}(\mathcal{P}_i)=(s_1,\ldots,s_i)$. Since $r_i<r_{i-1}$ and $s_i>s_{i-1}$, we have

$$\mathcal{U}_{r_i-1}\subset \mathcal{U}_{r_i}\subseteq \mathcal{U}_{r_{i-1}-1}\subseteq Q_{i-1}\cap P \tag{9}$$

and similarly

$$P+Q_{i-1}\subseteq \mathcal{W}_{\ell+s_{i-1}}\subseteq \mathcal{W}_{\ell+s_i-1}\subset \mathcal{W}_{\ell+s_i}. \tag{10}$$

First, we compute the number of possibilities for codimension one spaces U in Q_{i-1}, which will play the role of $Q_i\cap Q_{i-1}$, and then the number of possibilities in which to extend U to an ℓ-dimensional space satisfying $(a)-(d)$.

Keeping equation (9) and condition (c) in mind, we have that any such U should satisfy $\mathcal{U}_{r_i-1} \subseteq U$ but $\mathcal{U}_{r_i} \nsubseteq U$. Hence there are $\begin{bmatrix} \ell-r_i+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} \ell-r_i \\ 1 \end{bmatrix}_q = q^{\ell-r_i}$ many choices for U. Given one of these choices for U we choose $Q_i \in G_{\ell,m}$ containing U and satisfying $Q_i \subseteq \mathcal{W}_{\ell+s_i}$ but $Q_i \nsubseteq \mathcal{W}_{\ell+s_i-1}$. There are $\begin{bmatrix} s_i+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} s_i \\ 1 \end{bmatrix}_q = q^{s_i}$ many possibilities for Q_i. We claim that this Q_i satisfies $(a)-(d)$.

By construction $U \subset Q_i \cap Q_{i-1}$ and $Q_i \nsubseteq \mathcal{W}_{\ell+s_i-1}$. Since equation (10) implies $Q_{i-1} \subseteq \mathcal{W}_{\ell+s_i-1}$, we see that $Q_i \neq Q_{i-1}$. Hence $Q_i \cap Q_{i-1} = U$ and $\dim(Q_i \cap Q_{i-1}) = \ell - 1$. This proves (a).

Note that $U \cap P \subsetneq Q_{i-1} \cap P$, since $\mathcal{U}_{r_i} \nsubseteq U$, but $\mathcal{U}_{r_i} \subset Q_{i-1} \cap P$. Hence $\dim(U \cap P) \leq \ell - i$. On the other hand U is a hyperplane in Q_{i-1} and $U \cap P = U \cap (Q_{i-1} \cap P)$. Hence $\dim(U \cap P) \geq \dim(Q_{i-1} \cap P) - 1 = \ell - i$. We conclude $\dim(U \cap P) = \ell - i$. Clearly, $U \cap P \subseteq Q_i \cap P$, from which we see that $\dim(Q_i \cap P) \geq \ell - i$. We claim equality holds, which will prove (b). By construction $Q_i \subseteq \mathcal{W}_{\ell+s_i}$ but $Q_i \nsubseteq \mathcal{W}_{\ell+s_i-1}$. Hence $P + Q_i \subseteq \mathcal{W}_{\ell+s_i}$ but $P + Q_i \nsubseteq \mathcal{W}_{\ell+s_i-1}$. Since $U \subset Q_{i-1}$, from equation (10) we get $P + U \subseteq \mathcal{W}_{\ell+s_i-1}$ and hence we have $P + U \subsetneqq P + Q_i$. Consequently, $\dim(P + U) < \dim(P + Q_i)$. We have seen that $\dim(P \cap U) = \ell - i$ and therefore $\dim(P + U) = \ell + i - 1$. On the other hand, $\dim(P + Q_i) = 2\ell - \dim(P \cap Q_i)$. This implies $\dim(P \cap Q_i) < \ell - i + 1$ and we conclude that $\dim(P \cap Q_i) = \ell - i$. This proves (b).

To prove (c) we need to show that $\mathcal{U}_{r_i-1} \subseteq Q_i$ but $\mathcal{U}_{r_i} \nsubseteq Q_i$. The first part is clear as $\mathcal{U}_{r_i-1} \subset U \subseteq Q_i$. For the second part note that if $\mathcal{U}_{r_i} \subseteq Q_i$, then from equation (9) we get $\mathcal{U}_{r_i} \subseteq Q_i \cap Q_{i-1} = U$. However by construction $\mathcal{U}_{r_i} \nsubseteq U$. Hence $\mathcal{U}_{r_i} \nsubseteq Q_i$. This completes the proof of (c).

Finally, (d) follows by construction of Q_i as $Q_i \subseteq \mathcal{W}_{\ell+s_i}$ but $Q_i \nsubseteq \mathcal{W}_{\ell+s_i-1}$.

Combining the above, we see that there exist $q^{\ell-r_i+s_i}$ possibilities for Q_i. Hence there exist a set $\mathcal{L}(Q_{i-1}, r_i, s_i)$ of $q^{\ell-r_i+s_i-1}$ lines through Q_{i-1} with the desired properties. We fix an enumeration of these $q^{\ell-r_i+s_i-1}$ lines. If we choose another point $Q'_{i-1} \in \mathrm{Supp}(\omega) \setminus \{P\}$, we can use the argument to get a set $\mathcal{L}(Q'_{i-1}, r_i, s_i)$ of $q^{\ell-r_i+s_i-1}$ lines $L(U', W')$ in $G_{\ell,m}$ through Q'_{i-1} such that for any point Q'_i on $L(U', W')$ different from Q'_{i-1}, the corresponding sequence $\mathcal{P}'_i = (P, Q'_1, \ldots, Q'_{i-1}, Q'_i)$ is a geodesic from P to Q'_i satisfying $\mathbf{r}(\mathcal{P}'_i) = (r_1, \ldots, r_i)$ and $\mathbf{s}(\mathcal{P}'_i) = (s_1, \ldots, s_i)$. For each point Q'_i we also fix an enumeration of the $q^{\ell-r_i+s_i-1}$ lines.

Now we construct parity checks from ω as follows: for each $Q_{i-1} \in \mathrm{Supp}(\omega) \setminus \{P\}$ and $1 \leq a \leq q^{\ell-r_i+s_i-1}$, choose, using Theorem 2.7, a parity check $\omega_{a,Q_{i-1}}$ of $C(\ell, m)$ of weight three with support contained in the ath line of $\mathcal{L}(Q_{i-1}, r_i, s_i)$, such that the support of $\omega + \omega_{a,Q_{i-1}}$ does not contain Q_{i-1}. Like in the induction basis, we will do this in $\lfloor q/2 \rfloor$ different ways using a partition of the points on the ath line of $\mathcal{L}(Q_{i-1}, r_i, s_i)$ distinct from Q_{i-1}.

Then for each $1 \leq a \leq q^{\ell-r_i+s_i-1}$, we obtain $\lfloor q/2 \rfloor$ parity checks of the form

$$\eta(a,\omega) := \omega + \sum_{Q_{i-1}\in \mathrm{Supp}(\omega)\setminus\{P\}} \omega_{a,Q_{i-1}}.$$

First of all, note that $P \in \mathrm{Supp}(\eta(a,\omega))$ and $\mathrm{Supp}(\eta(a,\omega)) \setminus \{P\} \subset \overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$. Also note that by construction, property (2) is satisfied. Further, $|\mathrm{Supp}(\eta(a,\omega))| = 1 + 2^i$. Indeed no lines of $\mathcal{L}(Q_{i-1}, r_i, s_i)$ and $\mathcal{L}(Q'_{i-1}, r_i, s_i)$ can intersect each other. If they would intersect in a point, say Q, there would exist two distinct geodesics $\mathcal{P}_i$ and $\mathcal{P}'_i$ from P to Q both having i-tuples $\mathbf{r}$ and $\mathbf{s}$. But this is not possible by Theorem 3.12. Using a similar argument, we obtain that $\mathrm{Supp}(\eta(a,\omega)) \cap \mathrm{Supp}(\eta(a',\omega')) = \{P\}$ if $a \neq a'$ or $\omega \neq \omega'$. In particular $\eta(a,\omega)$ and $\eta(a',\omega')$ are mutually orthogonal on P if $a \neq a'$ or $\omega \neq \omega'$. If $a = a'$ and $\omega = \omega'$, but we used different sets of points from the partitions of the same lines in the sets $\mathcal{L}(Q'_{i-1}, r_i, s_i)$, then by construction the support of the corresponding parity checks only have P in common.

This proves (3). Finally, by construction and using the induction hypothesis, we have for given strictly monotonic $\mathbf{r} = (r_1, \ldots, r_i)$ and $\mathbf{s} = (s_1, \ldots, s_i)$, found exactly $\lfloor q/2 \rfloor^i \prod_{j=1}^{i} q^{\ell-r_j+s_j-1}$ parity checks. Adding over all possible such i-tuples and using Lemma 2.6, the result follows. □

Corollary 4.5. *Let $C(\ell, m)$ be a Grassmann code and let $P \in G_{\ell,m}$ be an arbitrary point. There exists a set $\mathcal{J}$ consisting of $J := \sum_{i=1}^{\ell} \left\lfloor \frac{q}{2} \right\rfloor^i q^{i^2-i} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q$ many parity checks for $C(\ell, m)$, which is orthogonal on the coordinate P. In particular, using majority logic decoding, we can correct up to $\lfloor \frac{J}{2} \rfloor$ errors.*

Proof. Let $P \in G_{\ell,m}$ be an arbitrary point. We define $\mathcal{J} := \cup_{i=1}^{\ell} \mathcal{J}_i$, where $\mathcal{J}_i$ are as in Theorem 4.4. Choose $1 \leq i \leq \ell$. By Theorem 4.4 the set of parity checks $\mathcal{J}_i$ is orthogonal on P. Since the support of the parity checks in $\mathcal{J}_i$ consists of P and a further 2^i points in $\overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$, they are orthogonal to the parity checks from $\mathcal{J}_t$ for any $t \neq i$. This proves that $\mathcal{J}$ is orthogonal on P. Using Theorem 4.4 again, we see that $|\mathcal{J}| = \sum_{i=1}^{\ell} |\mathcal{J}_i| = J$. Now the last part of the theorem follows from Theorem 4.2. □

Remark 4.6. In the construction of the set $\mathcal{J}$, many coordinate positions have been used. More precisely, since the parity checks in $\mathcal{J}_i$ have support in P and 2^i points of $\overline{P}^{(i)} \setminus \overline{P}^{(i-1)}$, the total number of points that occur in one of the parity checks in $\mathcal{J}$ equals:

$$1 + \sum_{i=1}^{\ell} 2^i \left\lfloor \frac{q}{2} \right\rfloor^i q^{i^2-i} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q.$$

If q is even, and in particular for binary Grassmann codes, then equations (5) and (6) imply that any point of $G_{\ell,m}$ occurs in the support of a parity check in $\mathcal{J}$. Hence the set $\mathcal{J}$ cannot be extended further for even q.

Remark 4.7. As Example 4.3 shows, the majority logic decoder from Corollary 4.5 does not in general decode up to half the minimum distance of $C(\ell, m)$. Let us investigate more closely what happens. If $\ell = 1$, then $C(1, m)$ is an $[n, k, d] = [(q^m - 1)/(q - 1), m, q^{m-1}]$ code. In fact it is a first order projective Reed–Muller code. We have $J = \lfloor q/2 \rfloor \begin{bmatrix} 1 \\ 1 \end{bmatrix}_q \begin{bmatrix} m-1 \\ 1 \end{bmatrix}_q = \lfloor q/2 \rfloor (q^{m-1} - 1)/(q-1)$. Hence in the binary case, we decode up to half the minimum distance, while for large q we can correct up to roughly $d/4$ errors.

More generally, if ℓ and m are fixed and q tends to infinity, then it easy to see that $J/d \to 1/2^\ell$. Hence for large q we can correct up to $d/2^{\ell+1}$ many errors using Corollary 4.5. If ℓ and q are fixed, but m tends to infinity, a direct calculation shows that $\lim_{m\to\infty} J/d = M_q(\ell)/2^\ell$, where $M_q(\ell)$ is as in equation (2). Note that $M_q(\ell) > 1$ if q is even, while $M_q(\ell) < 1$ if q is odd. It is not surprising that the case q is even performs better than the odd case, since for even q, we have used all points of $G_{\ell,m}$ in the support of some parity check in $\mathcal{J}$, while for odd q there are points that do not appear in the support of any parity check in $\mathcal{J}$. The following small table gives an impression on what happens for small values of q, ℓ, and m.

q	2	2	2	2	2	2	3	3	3	4	4
ℓ	2	2	2	2	3	3	2	2	2	2	2
m	4	5	6	7	6	7	4	5	6	4	5
J	13	49	185	713	309	2045	25	169	1330	114	1554
d	16	64	256	1024	512	4096	81	729	6561	256	4096

Remark 4.8. Note that any one-step majority logic decoder is fast to execute. In our case, the computation of a parity check from $\mathcal{J}_i$ costs 2^i multiplications in $\mathbb{F}_q$. Therefore, to carry out the majority voting for a single coordinate $P \in G_{\ell,m}$ costs N multiplications in $\mathbb{F}_q$, where

$$N = \sum_{i=1}^{\ell} 2^i \left\lfloor \frac{q}{2} \right\rfloor^i q^{i^2-i} \begin{bmatrix} \ell \\ i \end{bmatrix}_q \begin{bmatrix} m-\ell \\ i \end{bmatrix}_q .$$

Note that $N \leq |G_{\ell,m}| - 1$, since $|G_{\ell,m}|$ is the length n of the code $C(\ell, m)$ and for each coordinate different from P, at most one multiplication needs to be carried out. Performing the majority logic decoding on all coordinates therefore takes at most $n(n-1)$ multiplications in $\mathbb{F}_q$. In this model, we assumed that for each coordinate, the used set of orthogonal parity check on that coordinate was stored in memory. For a given coordinate P, the memory requirement would be of the order of magnitude of n: one would need to store the support sets of the used parity checks, i.e., essentially a partition of the $n-1$ coordinates distinct from P, and for each coordinate a value from $\mathbb{F}_q$ to indicate the coordinates of the parity checks. Hence the total memory requirement would be of the order of magnitude n^2.

The memory requirement can easily be reduced. If we only store the set of orthogonal parity checks on one fixed coordinate P, we could apply an automorphism of the Grassmannian to obtain the required sets of orthogonal parity checks

on the other coordinates. As explained in Section 2, the n points of $G_{\ell,m}$ can be represented by certain $\ell \times m$ matrices, which we may assume to be in row-reduced echelon form. Applying an automorphism then boils down to multiplying these n matrices with a suitable $m \times m$ matrix, after which the result should be brought in row-reduced echelon form again. This would cost around $\ell m^2 n$ operations using naive matrix multiplication algorithms. The $m \times m$ matrix could be stored in memory. Doing this for all coordinates, would give rise to a cost of $m^2 n$ in memory to store the needed $m \times m$ matrices, while the computational cost would be $\ell m^2 n^2$. Since m and ℓ are at best logarithmic in n, this would not increase the running time of the decoder by much, while the memory requirement would be reduced significantly.

Grassmann codes have been decoded in the literature before. Kroll–Vincenti have studied permutation decoding for the codes $C(1,4)$, $C(1,5)$, and $C(2,4)$ [14]. Ghorpade–Piñero [10] have extended this approach to affine Grassmann codes [1], which are codes that can be seen as Grassmann codes that have been punctured in $\begin{bmatrix} m \\ \ell \end{bmatrix}_q - q^{\ell(m-\ell)}$ coordinate positions. The algorithm in [10] can decode up to $d/\binom{m}{\ell} - 1$ errors and although a complexity analysis was not given, it seems that their algorithm uses around kn^2 multiplications in $\mathbb{F}_q$.

Let us compare our decoding algorithm with theirs. First of all, the complexity of our algorithm is slightly better. Moreover, if ℓ and q are fixed, but m tends to infinity, their error-correcting radius will tend to zero, while we have seen that ours tends to $M_q(\ell)/2^{\ell+1} > 0$. Note $\binom{m}{\ell} > 2^{\ell+1}$ for every $\ell \geq 3$, or $\ell = 2$ and $m \geq 5$, or $\ell = 1$ and $m \geq 5$. Hence if ℓ and m are fixed, but q tends to infinity, our algorithm performs better as well.

5. Acknowledgements

Peter Beelen would like to acknowledge the support from The Danish Council for Independent Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B.

Prasant Singh would like to thank HC rsted-COFUND postdoctoral grant *Understanding Schubert Codes*. Most of the work of this article was done when he was working under this project at DTU, Denmark. He would also like to express his gratitude to the Indo-Norwegian project supported by RCN, Norway (Project number 280731), and the DST of Govt. of India.

References

[1] P. Beelen, S.R. Ghorpade and T. Høholdt, Affine Grassmann codes, *IEEE Trans. Inform. Theory* **56** (2010), 3166–3176.

[2] P. Beelen, S.R. Ghorpade and T. Høholdt, Duals of affine Grassmann codes and their relatives, *IEEE Trans. Inform. Theory* **58** (2012), 3843–3855.

[3] P. Beelen and F. Piñero, The structure of dual Grassmann codes, *Des. Codes Cryptogr.* **79** (2016), 451–470.

[4] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance regular graphs, Springer, 1989.

[5] F. Buekenhout and A.M. Cohen, Diagram Geometry: Related to Classical Groups and Buildings, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics, 57. Springer, Heidelberg, 2013.

[6] W.L. Chow, On the geometry of algebraic homogeneous spaces, *Ann. of Math.***(2) 50** (1949), 32–67.

[7] S.R. Ghorpade and K.V. Kaipa, Automorphism groups of Grassmann codes, *Finite Fields Appl.* **23** (2013), 80–102.

[8] S.R. Ghorpade and G. Lachaud, Higher weights of Grassmann codes, *Coding Theory, Cryptography and Related Areas* (Guanajuato, 1998), J. Buchmann, T. Hoeholdt, H. Stichtenoth and H. Tapia-Recillas Eds., Springer-Verlag, Berlin, (2000), 122–131.

[9] S.R. Ghorpade, A.R. Patil and H.K. Pillai, Decomposable subspaces, linear sections of Grassmann varieties, and higher weights of Grassmann codes, *Finite Fields Appl.* **15** (2009), 54–68.

[10] S.R. Ghorpade and F.L. Piñero, Information set and iterative encoding for Affine Grassmann codes, *Proceedings 2015 Seventh International Workshop on Signal Design and its Applications in Communications* (IWSDA 2015), 175–179.

[11] S.R. Ghorpade and M.A. Tsfasman, Schubert varieties, linear codes and enumerative combinatorics, *Finite Fields Appl.* **11** (2005), 684–699.

[12] K. Kaipa and H. Pillai, Weight spectrum of codes associated with the Grassmannian $G(3,7)$, *IEEE Trans. Inform. Theory* **59** (2013), 983–993.

[13] S.L. Kleiman and D. Laksov, Schubert calculus, *Amer. Math. Monthly* **79** (1972), 1061–1082.

[14] H.J. Kroll and R. Vincenti, PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of PG(5,2), *Discrete Math.* **308** (2008), 408-414.

[15] S. Lin and D.J. Costello Jr., Error Control Coding, Pearson Prentice Hall, 1983.

[16] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error Correcting Codes, Elsevier, New York, 1977.

[17] L. Manivel, Symmetric functions, Schubert polynomials and degeneracy loci. Translated from the 1998 French original by John R. Swallow. SMF/AMS Texts and Monographs, 6. Cours Spcialiss [Specialized Courses], 3. American Mathematical Society, Providence, RI; Socit Mathmatique de France, Paris, 2001.

[18] J.L. Massey, Threshold decoding, Massachusetts Institute of Technology, Research Laboratory of Electronics, Tech. Rep. 410, Cambridge, Mass., 1963.

[19] D.Yu. Nogin, Codes associated to Grassmannians, *Arithmetic, Geometry and Coding Theory* (Luminy, 1993), R. Pellikaan, M. Perret, S. G. Vlăduţ, Eds., Walter de Gruyter, Berlin, (1996), 145–154.

[20] D.Yu. Nogin, The spectrum of codes associated with the Grassmannian variety $G(3,6)$, *Problems of Information Transmission* **33** (1997), 114–123

[21] M. Pankov, Grassmannians of Classical Buildings, World Scientific, 2010.

[22] M. Pankov, Wigner-Type Theorems for Hilbert Grassmannians, Cambridge University Press, 2020.

[23] C.T. Ryan, An application of Grassmannian varieties to coding theory, *Congr. Numer.* **157** (1987), 257–271.

[24] C.T. Ryan, Projective codes based on Grassmann varieties, *Congr. Numer.* **157** (1987), 273–279.

[25] E.E. Shult, Points and lines. Characterizing the classical geometries. Universitext. Springer, Heidelberg, 2011.

[26] D. Silva and F.R. Kschischang, On Metrics for Error Correction in Network Coding, *IEEE Trans. Inform. Theory* **55** (2009), 5479–5490.

[27] M. Tsfasman, S. Vladut and D. Nogin, Algebraic Geometric Codes: Basic Notions, Mathematical Surveys and Monographs, 139. American Mathematical Society, Providence, RI, 2007.

Department of Applied Mathematics and Computer Science,
Technical University of Denmark,
Matematiktorvet 303B, 2800 Kgs. Lyngby, Denmark.
E-mail address: pabe@dtu.dk

Department of Mathematics and Statistics,
University of Tromsø,
Hansine Hansens veg 18, 9019, Norway.
E-mail address: psinghprasant@gmail.com