

SOME RESULTS ON SUBSPACE ARRANGEMENT CODES AND CRYPTOSYSTEMS

MIDN 2/C JAMES BERG

1. PROJECT OVERVIEW

What follows is just one facet of a Trident Scholar project, with input from work done in the SM450A class. The overall goal of the project is to build and develop a class of efficient error-correcting codes through recent advances in the algebraic geometry, combinatorics, and commutative algebra of subspace arrangements. These codes are evaluation codes, which are constructed using an ideal on a polynomial ring. The results that follow deal with one specific ideal, namely, $I = \langle x_1 \cdots x_l \rangle$ in the polynomial ring $\mathbb{F}_q[x_1, \dots, x_l]$ in relation to the vector space \mathbb{F}_q^l (note that \mathbb{F}_q is a finite field). Furthermore, note that in the construction of these codes, in order to form a basis for the code, all polynomials up to degree j (which is selected beforehand) are evaluated on each point in the vector space which evaluates to zero on the ideal. There are two components to this component of the project: a short segment on the relationship of the subspace arrangement codes being constructed for the Trident Scholar project to Reed-Muller codes, and then a longer section describing some results with regard to the dimension, k , of a code based upon the ideal $I = \langle x_1 \cdots x_l \rangle$. The sage file attached to this report was instrumental in these conclusions since it was able to easily generate properties of parts of the matrix that represent the code.

2. REED-MULLER CODES AND HYPERPLANE ARRANGEMENTS

2.1. Description of Reed-Muller codes and Properties. Reed-Muller codes are a class of codes that are closely related to the subspace arrangement codes used in this project. Just as an ideal is used to generate a subspace arrangement code, a Reed-Muller code can be interpreted as developing from the ideal $I = \langle 0 \rangle$. Consequently, the construction and properties of subspace arrangement codes can be applied to Reed Muller codes with $I = \langle 0 \rangle$ (essentially, all points are considered in the matrix construction because $I = \langle 0 \rangle$). Thus, formulae for the length (n), dimension (k), and minimum distance (d) of certain types of Reed-Muller codes can be given. Citing *Introduction to Coding Theory* by Jacobus Hendricus van Lint, when $q = 2$, $n = 2^l$, $k = \sum_{s=0}^j \binom{l}{s}$, and $d = 2^{l-j}$. In general, $n = q^l$, since, as stated earlier, all points in the vector space are considered. Further formulae for other instances of q are currently not known or publicized, but, if $j < q$, $d = (q - j)q^{l-1}$, according to *List Decoding of q-ary Reed-Muller Codes* by Raad Pellikaan and Xin-Wen Wu.

2.2. Conjectures Based upon Reed-Muller Codes. Using the Sage file and functions developed and used by Professor Joyner, Professor Wakefield, and myself, numerous examples of Reed-Muller codes and subspace arrangement codes based upon the ideal $I = \langle x_1 \cdots x_l \rangle$ were generated (j , l , and q where held constant for each pairing of a Reed-Muller code and a subspace arrangement code). Though no definitive results were given, some trends were identified, and they are listed here. Let $n = q^l$, $k = k_{GR-M}$, and $d = d_{GR-M}$ for the generalized

Reed-Muller code. For selections of $q, l, j \leq l-1$, and $I = \langle x_1 \cdots x_l \rangle$, $n = q^l - (q-1)^l$ (this number represents all points that have at least one 0 component [so they are on a hyperplane], obtained by subtracting the number of non-zero elements raised to the number of positions in a point from the number of all points). Furthermore, there are indications that, for the subspace arrangement code, $k = k_{GR-M}$ and $d = d_{GR-M} - (q-1)^l$. If $j = l$, n clearly remains the same; on the other hand, it appears that $k = \dim(\text{Generalized Reed-Muller code}) - 1$ and $d = d_{GR-M} - (q-1)^l$. Ideally, these formulae can be proven, as well as finding formulae for the dimension and minimum distance of any generalized Reed-Muller Code.

3. PROOFS REGARDING THE DIMENSION OF CODES GENERATED BY THE IDEAL

$$I = \langle x_1 \cdots x_l \rangle$$

3.1. Dimension for $I = \langle x_1 \cdots x_l \rangle$ whenever $j = 1$: $k = l + 1$. Previous work allowed the extension of a theorem by Richard Stanley to be applied to this class of error-correcting codes, establishing an upper bound for dimension: $k \leq \sum_{m=0}^j \binom{m+l-1}{m} = \sum_{m=0}^l \binom{m+l-1}{m} = \binom{l-1}{0} + \binom{l}{1} = l + 1$. The dimension of $l + 1$ refers to the number of linearly independent row vectors produced by the matrix construction of the *Eval* function for generating the code. Each row corresponds to a polynomial. Thus, the polynomials are $1, x_1, \dots, x_l$. Thus, it suffices to show that the row vectors $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_l$ produced by the respective polynomials $1, x_1, \dots, x_l$ are linearly independent. Define e_i as the point $(0, 0, \dots, 0, 1, 0, \dots, 0)$ in \mathbb{F}_q^l such that all components in e_i are 0 except for the i th position. Furthermore, define e_0 as the origin, $(0, 0, \dots, 0, \dots, 0)$. Note that regardless of the selection of q , e_i for $i = 0, \dots, l$ all evaluate to 0 on I , so $e_i \in V(I)$, $i = 0, \dots, l$. For simplicity (but without loss of generality), let e_0, \dots, e_l correspond to the first $l + 1$ columns in the matrix. To show linear independence, let $\mathbf{L} = c_0 \mathbf{v}_0 + c_1 \mathbf{v}_1 + \cdots + c_l \mathbf{v}_l = \mathbf{0}$. Define $\mathbf{v}_i(j)$ as the j th position in the i th vector, where the initial position and vector are defined respectively as e_0 and \mathbf{v}_0 . $\mathbf{L}(i)$ is defined similarly. Examine $\mathbf{L}(0) = c_0 \mathbf{v}_0(0) + c_1 \mathbf{v}_1(0) + \cdots + c_l \mathbf{v}_l(0) = 0$, which simplifies to $c_0(1) + c_1(0) + \cdots + c_l(0) = c_0(1) = c_0 = 0$. Thus, $c_0 = 0$, so it suffices to only examine $\mathbf{L}' = c_1 \mathbf{v}_1 + \cdots + c_l \mathbf{v}_l = \mathbf{0}$. Note that for all $i > 0$, $\mathbf{L}'(i) = c_1 \mathbf{v}_1(i) + \cdots + c_l \mathbf{v}_l(i) = c_1(0) + \cdots + c_i(1) + \cdots + c_l(0) = c_i(1) = c_i = 0$, so $c_i = 0$ for all $i > 0$. Hence, the only solution to $\mathbf{L} = c_0 \mathbf{v}_0 + c_1 \mathbf{v}_1 + \cdots + c_l \mathbf{v}_l = \mathbf{0}$ is the trivial solution $c_0 = c_1 = \cdots = c_i = \cdots = c_l = 0$, meaning that $\{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_l\}$ are linearly independent. Therefore, each of the $l + 1$ row vectors in the matrix are linearly independent, so $k = l + 1$. \square

3.2. Dimension for $I = \langle x_1 x_2 \rangle$ whenever $q > 2$, $j = l = 2$: $k = 5$. Since $q > 2$, \mathbb{F}_q^2 contains at least 3 elements, $0, 1, \omega$. In the matrix construction, let the first 5 columns correspond to the points $(0, 0), (1, 0), (0, 1), (\omega, 0), (0, \omega)$, and the rows correspond to the polynomials $1, x_1, x_2, x_1^2, x_2^2$. Note that these are 5 of the 6 polynomials covered by the upper bound (which is $\sum_{m=0}^j \binom{m+l-1}{m} = \sum_{m=0}^2 \binom{m+1}{m} = \binom{1}{0} + \binom{2}{1} + \binom{3}{2} = 6$; the polynomial not used is $x_1 x_2$ since all points in $V(I)$ have at least one term a 0, so $x_1 x_2$ evaluates to 0 for all points in $V(I)$, creating a linearly dependent row vector in the matrix). Thus, the resulting matrix

is as follows:

$$\begin{array}{cccccc}
 & (0,0) & (1,0) & (0,1) & (\omega,0) & (0,\omega)\dots \\
 1 & 1 & 1 & 1 & 1 & 1\dots \\
 x_1 & 0 & 1 & 0 & \omega & 0\dots \\
 x_2 & 0 & 0 & 1 & 0 & \omega\dots \\
 x_1^2 & 0 & 1 & 0 & \omega^2 & 0\dots \\
 x_1^2 & 0 & 0 & 1 & 0 & \omega^2\dots
 \end{array}$$

Since, by both examination of the matrix and by a parallel argument to the first proof, the first row is linearly independent from the other four, only the four other row vectors need to be shown to be linearly independent. Furthermore, the first column vector, which becomes all 0s in the absence of the first row vector, can also be removed. To show linear independence the determinant of the resulting matrix can be taken (only 4 columns need be considered), which is as follows:

$$\begin{array}{cccc}
 & (1,0) & (0,1) & (\omega,0) & (0,\omega) \\
 x_1 & 1 & 0 & \omega & 0 \\
 x_2 & 0 & 1 & 0 & \omega \\
 x_1^2 & 1 & 0 & \omega^2 & 0 \\
 x_1^2 & 0 & 1 & 0 & \omega^2
 \end{array}$$

The determinant of the matrix is $\omega^2(\omega-1)^2 \neq 0$ since \mathbb{F}_q is a field and thus an integral domain, meaning it has no zero divisors (note to that $\omega \neq 0, \omega \neq 1$). Thus, all 5 row vectors of the original matrix construction are linearly independent, implying that the dimension of the code is 5. \square

3.3. Dimension for $I = \langle x_1x_2x_3 \rangle$ whenever $q > 2, j = 2, l = 3: k = 10$. First note that 10 corresponds to the upper bound: $\sum_{m=0}^j \binom{m+l-1}{m} = \sum_{m=0}^2 \binom{m+2}{m} = \binom{2}{0} + \binom{3}{1} + \binom{4}{2} = 10$, corresponding to the polynomials $1, x_1, x_2, x_3, x_1^2, x_2^2, x_3^2, x_1x_2, x_1x_3, x_2x_3$. Thus, carefully selecting the points in $V(I)$ in the columns (which can be ordered in any way), a part of the matrix can be constructed (note that since $q > 2, 0, 1, \omega$ are at least in \mathbb{F}_q):

$$\begin{array}{cccccccccc}
 & (0,0,0) & (1,0,0) & (0,1,0) & (0,0,1) & (\omega,0,0) & (0,\omega,0) & (0,0,\omega) & (1,\omega,0) & (1,0,\omega) & (0,1,\omega)\dots \\
 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\dots \\
 x_1 & 0 & 1 & 0 & 0 & \omega & 0 & 0 & 1 & 1 & 0\dots \\
 x_2 & 0 & 0 & 1 & 0 & 0 & \omega & 0 & \omega & 0 & 1\dots \\
 x_3 & 0 & 0 & 0 & 1 & 0 & 0 & \omega & 0 & \omega & \omega\dots \\
 x_1^2 & 0 & 1 & 0 & 0 & \omega^2 & 0 & 0 & 1 & 1 & 0\dots \\
 x_1^2 & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & \omega^2 & 0 & 1\dots \\
 x_3^2 & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & \omega^2 & \omega^2\dots \\
 x_1x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0\dots \\
 x_1x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & 0\dots \\
 x_2x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega\dots
 \end{array}$$

As in the last example, the first row is linearly independent of the other 9, so it (and the first column) can be removed. Furthermore, note that the last three rows are linearly independent from the other remaining 6 since their first 6 terms are 0, whereas no other row vectors exhibit

this property. Furthermore, the last three are linearly independent by examining the bottom-right 3-by-3 matrix,

$$\begin{array}{ccc} & (1, \omega, 0) & (1, 0, \omega) & (0, 1, \omega) \\ x_1 x_2 & \omega & 0 & 0 \\ x_1 x_3 & 0 & \omega & 0 \\ x_2 x_3 & 0 & 0 & \omega \end{array} .$$

Thus, all that must be examined is the six remaining row vectors; the last 3 columns listed can also be disregarded since they are only necessary to show that the last three row vectors are linearly independent. All that remains is a 6-by-6 matrix:

$$\begin{array}{cccccc} & (1, 0, 0) & (0, 1, 0) & (0, 0, 1) & (\omega, 0, 0) & (0, \omega, 0) & (0, 0, \omega) \\ x_1 & 1 & 0 & 0 & \omega & 0 & 0 \\ x_2 & 0 & 1 & 0 & 0 & \omega & 0 \\ x_3 & 0 & 0 & 1 & 0 & 0 & \omega \\ x_1^2 & 1 & 0 & 0 & \omega^2 & 0 & 0 \\ x_1^2 & 0 & 1 & 0 & 0 & \omega^2 & 0 \\ x_3^2 & 0 & 0 & 1 & 0 & 0 & \omega^2 \end{array} ,$$

which has a determinant of $\omega^3(\omega - 1)^3 \neq 0$ since there are no zero divisors in \mathbb{F}_q . Therefore, the middle six row vectors are linearly independent, which are linearly independent from the last three row vectors (which are also linearly independent), all of which are linearly independent from the first row vector. Thus, there are 10 linearly independent row vectors in the matrix construction, implying that the dimension of the code is 10. \square

3.4. Dimension for $I = \langle x_1 \cdots x_l \rangle$ whenever $q > 2$, $j = 2$, $l \geq 3$: $k = \frac{l^2+l}{2} + l + 1$. First

note that $k = \frac{l^2+l}{2} + l + 1$ corresponds to the upper bound, $\sum_{m=0}^j \binom{m+l-1}{m} = \sum_{m=0}^2 \binom{m+l-1}{m} = \binom{l-1}{0} + \binom{l-1}{1} + \binom{l-1}{2} = 1 + l + \frac{(l-1)!}{(l-1)!2} = 1 + l + \frac{(l-1)(l)}{2} = \frac{l^2+l}{2} + l + 1$. Notice that since this is the upper bound, the proposed dimension corresponds to all polynomials in \mathbb{F}_q^l of degree 0, 1, and 2. Thus, it is sufficient to show that all $\frac{l^2+l}{2} + l + 1$ rows in the matrix construction of the code are linearly independent. The matrix can be constructed as follows:

$$\begin{array}{cccccccccccc} & (0, \dots, 0) & (1, 0, \dots, 0) & \dots & (0, \dots, 0, 1) & (\omega, 0, \dots, 0) & \dots & (0, \dots, 0, \omega) & (1, \omega, 0, \dots, 0) & \dots & (1, 0, \dots, 0, \omega) & \dots & (0, \dots, 0, 1, \omega) \dots \\ x_1 & 1 & 0 & \dots & 1 & \omega & \dots & 1 & 1 & \dots & 1 & \dots & 1 \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \dots \\ x_l & 0 & 0 & \dots & 1 & 0 & \dots & \omega & 0 & \dots & \omega & \dots & \omega \dots \\ x_l^2 & 0 & 1 & \dots & 0 & \omega^2 & \dots & 0 & 1 & \dots & 1 & \dots & 0 \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \dots \\ x_l^2 & 0 & 0 & \dots & 1 & 0 & \dots & \omega^2 & 0 & \dots & \omega^2 & \dots & \omega^2 \dots \\ x_1 x_2 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \omega & \dots & 0 & \dots & 0 \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \dots \\ x_1 x_l & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & \omega & \dots & 0 \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \dots \\ x_{l-1} x_l & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & \omega \dots \end{array} .$$

To parallel the argument for the specific case of $l = 3$, note that the first row vector is linearly independent from the others since it is the only row vector with a 1 as its first entry. Additionally, all polynomials which are the product of two distinct first-degree polynomials are linearly independent from the other row vectors since the first $2l + 1$ columns are zero. Additionally, these row vectors are linearly independent since the ensuing $\binom{l}{2}$ columns

$((1, \omega, 0, \dots, 0) \dots (0, \dots, 0, 1, \omega))$ where chosen such that the corresponding polynomial in representing the row vector evaluates to ω , thereby forming a smaller $\binom{l}{2}$ by $\binom{l}{2}$ matrix with ω in each diagonal entry and 0s elsewhere, thereby making each of these row vectors linearly independent. Thus, all that is left to be shown to be linearly independent are the row vectors corresponding to the polynomials $x_1, \dots, x_l, x_1^2, \dots, x_l^2$. Note that the collection of row vectors corresponding to the polynomials x_1, \dots, x_l are linearly independent since (removing the first column) an upper triangular matrix with 1 in each diagonal entry is formed; the same is true for the row vectors corresponding to x_1^2, \dots, x_l^2 . Note that the first group of l row vectors are linearly independent from the second group of l row vectors since (letting x_i and x_i^2 represent each group, where x_i is arbitrarily chosen) the row vectors corresponding to x_i and x_i^2 are identical (after deleting the first column) in the first l columns, but differ in the ensuing l columns (note that a square matrix can be made deleting the first column and all columns after the column corresponding to $(0, \dots, 0, \omega)$). Thus, the determinant of such a square matrix must be nonzero, and, within the matrix, no row vector is a multiple (and thus not a linear combination) of any other row. Therefore, these $2l$ vectors must be linearly independent. Therefore, all of the row vectors (all $1 + \binom{l}{2} + 2l = \frac{l^2+1}{2} + l + 1$ of them) in the matrix must be linearly independent. \square

3.5. Dimension for $I = \langle x_1x_2x_3x_4 \rangle$, whenever $j = 3, q > 3, l = 4: k = 35$. Of first note is the upper bound for these parameters: $k \leq \sum_{m=0}^j \binom{m+l-1}{m} = \sum_{m=0}^3 \binom{m+3}{m} = \binom{3}{0} + \binom{4}{1} + \binom{5}{2} + \binom{6}{3} = 1 + 4 + 10 + 20 = 35$. Thus, in order to show that the dimension is 35, it suffices to show that each row vector in the matrix construction of the code (of which there are 35 for each polynomial of degree less than or equal to 3) is linearly independent. Furthermore, careful ordering of the columns of the matrix construction will lend themselves to a clear determination of linear independence. Thus, the matrix construction can be as follows (note that since $q > 3, \{0, 1, \omega, \omega^2\}$ are all at least in \mathbb{F}_q^3):

| | | | | | | | | | | | | | | |
|-------------|-----------|-----------|-----------|-----------|-----------|--------------------|--------------------|--------------------|--------------------|----------------------|----------------------|----------------------|----------------------|-----|
| | (0,0,0,0) | (1,0,0,0) | (0,1,0,0) | (0,0,1,0) | (0,0,0,1) | (ω ,0,0,0) | (0, ω ,0,0) | (0,0, ω ,0) | (0,0,0, ω) | (ω^2 ,0,0,0) | (0, ω^2 ,0,0) | (0,0, ω^2 ,0) | (0,0,0, ω^2) | ... |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ... |
| x_1 | 0 | 1 | 0 | 0 | 0 | ω | 0 | 0 | 0 | ω^2 | 0 | 0 | 0 | ... |
| x_2 | 0 | 0 | 1 | 0 | 0 | 0 | ω | 0 | 0 | 0 | ω^2 | 0 | 0 | ... |
| x_3 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ω | 0 | 0 | 0 | ω^2 | 0 | ... |
| x_4 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ω | 0 | 0 | 0 | ω^2 | ... |
| x_1^2 | 0 | 1 | 0 | 0 | 0 | ω^2 | 0 | 0 | 0 | ω^4 | 0 | 0 | 0 | ... |
| x_2^2 | 0 | 0 | 1 | 0 | 0 | 0 | ω^2 | 0 | 0 | 0 | ω^4 | 0 | 0 | ... |
| x_3^2 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ω^2 | 0 | 0 | 0 | ω^4 | 0 | ... |
| x_4^2 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ω^2 | 0 | 0 | 0 | ω^4 | ... |
| x_1^3 | 0 | 1 | 0 | 0 | 0 | ω^3 | 0 | 0 | 0 | ω^6 | 0 | 0 | 0 | ... |
| x_2^3 | 0 | 0 | 1 | 0 | 0 | 0 | ω^3 | 0 | 0 | 0 | ω^6 | 0 | 0 | ... |
| x_3^3 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ω^3 | 0 | 0 | 0 | ω^6 | 0 | ... |
| x_4^3 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | ω^3 | 0 | 0 | 0 | ω^6 | ... |
| x_1x_2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | ... |
| $x_2x_3x_4$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |

Note that all polynomials which have the multiplication $x_i x_j$ ($j \neq i$) as a factor evaluate to 0 upon all of these listed points. Thus, the linear independence of the row vectors associated with those polynomials is not contingent upon the linear independence of the first 13 row vectors. Furthermore, note that the row vector associated with the constant polynomial is the only row vector with a non-zero element as the initial element; thus it is linearly independent from the other 34 row vectors and need not be considered in any further arguments. Thus, the second through thirteenth row vectors can be considered one case. In order to show the linear

independence of these row vectors, the determinant of the following matrix must be shown to be non-zero (the matrix consists of the components of the second through thirteenth rows and columns of the previous matrix):

$$\begin{array}{cccccccccccc}
 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 \\
 1 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^4 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^4 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^4 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^4 \\
 1 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 & \omega^6 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 & \omega^6 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 & \omega^6 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 & \omega^6
 \end{array} .$$

Row-reduction techniques will allow the creation of an upper triangular matrix, which has a determinant that is easy to calculate. Let the first four rows of the above matrix be collective called \mathbf{A} , the next four \mathbf{B} , and the last four \mathbf{C} . Let operations $c\mathbf{A} + d\mathbf{B}$ be defined as the multiplication of each row in \mathbf{A} and \mathbf{B} by c and d , respectively and then the component-wise addition of \mathbf{A} and \mathbf{B} (so the first row in \mathbf{A} is added to the first row in \mathbf{B} ; this is analogous to creating a new vector space). Thus, (through row-reduction) replace \mathbf{B} by $\mathbf{B} - \mathbf{A}$, and replace \mathbf{C} by $\mathbf{C} - \mathbf{B} - \omega(\mathbf{B} - \mathbf{C})$:

$$\begin{array}{cccccccccccc}
 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & 0 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & 0 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 \\
 0 & 0 & 0 & 0 & \omega^2 - \omega & 0 & 0 & 0 & \omega^4 - \omega^2 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & \omega^2 - \omega & 0 & 0 & 0 & \omega^4 - \omega^2 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 - \omega & 0 & 0 & 0 & \omega^4 - \omega^2 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 - \omega & 0 & 0 & 0 & \omega^4 - \omega^2 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^6 - \omega^5 - \omega^4 + \omega^3 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^6 - \omega^5 - \omega^4 + \omega^3 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^6 - \omega^5 - \omega^4 + \omega^3 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^6 - \omega^5 - \omega^4 + \omega^3
 \end{array} .$$

Note that this is an upper triangular matrix, so the determinant of it is the product of the diagonal entries: $1^4(\omega^2 - \omega)^4(\omega^6 - \omega^5 - \omega^4 + \omega^3)^4 = \omega^4(\omega - 1)^4(\omega^3((\omega - 1)(\omega + 1)(\omega - 1)))^4 = \omega^{16}(\omega - 1)^{12}(\omega + 1)^4$. Thus, the determinant is 0 if and only if $\omega = 0, 1, -1$. However, since $q > 3$, ω does not take on any of these values ($\{0, 1, \omega, \omega^2\}$ are all distinct, ruling out $\omega = 0, 1$; if $\omega = -1$, then $\omega^2 = (-1)^2 = 1$, another contradiction). Therefore, the determinant of the matrix is non-zero for $q > 3$, implying that all of these row vectors are linearly independent. Thus, all that must be shown is the remaining 22 row vectors to be linearly independent. Note that for the remaining 22 row vectors, each falls into two categories: corresponding to polynomials either consisting of two or three multiplications among two terms (there are 18 such vectors) or to three multiplications among three terms (there 4 such vectors). These categories can be considered different from each other since, if all 22 of the corresponding polynomials are evaluated on points on a coordinate 2-dimensional plane in \mathbb{F}_q^4 (so there are 2 0s in each point), all of the polynomials in the latter category would always be zero while those in the former would be non-zero on some point. Thus, the latter group can be isolated

from the other 31 row vectors in the following matrix:

$$\begin{array}{cccc}
 & (1, 1, 1, 0) & (1, 1, 0, 1) & (1, 0, 1, 1) & (0, 1, 1, 1) \\
 x_1x_2x_3 & 1 & 0 & 0 & 0 \\
 x_1x_2x_4 & 0 & 1 & 0 & 0 \\
 x_1x_3x_4 & 0 & 0 & 1 & 0 \\
 x_2x_3x_4 & 0 & 0 & 0 & 1
 \end{array}$$

Clearly, these 4 vectors are linearly independent among each other and thus among all 35 row vectors. Hence, only the remaining 18 vectors need be examined. Examine the following matrix of the remaining 18:

$$\begin{array}{cccccccccccccccccccc}
 & 1100 & 1010 & 1001 & 0110 & 0101 & 0011 & 1\omega00 & 10\omega0 & 100\omega & 01\omega0 & 010\omega & 001\omega & \omega\omega^200 & \omega0\omega^20 & \omega00\omega^2 & 0\omega\omega^20 & 0\omega0\omega^2 & 00\omega\omega^2 \\
 x_1x_2 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 & 0 & 0 \\
 x_1x_3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 & 0 \\
 x_1x_4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^3 & 0 & 0 & 0 \\
 x_2x_3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^3 & 0 & 0 \\
 x_2x_4 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^3 & 0 \\
 x_3x_4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^3 \\
 x_1^2x_2 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^4 & 0 & 0 & 0 & 0 & 0 \\
 x_1^2x_3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^4 & 0 & 0 & 0 & 0 \\
 x_1^2x_4 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^4 & 0 & 0 & 0 \\
 x_2^2x_3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^4 & 0 & 0 \\
 x_2^2x_4 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^4 & 0 \\
 x_3^2x_4 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^4 \\
 x_1x_2^2 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & \omega^5 & 0 & 0 & 0 & 0 & 0 \\
 x_1x_3^2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & \omega^5 & 0 & 0 & 0 & 0 \\
 x_1x_4^2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & \omega^5 & 0 & 0 & 0 \\
 x_2x_3^2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & \omega^5 & 0 & 0 \\
 x_2x_4^2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & \omega^5 & 0 \\
 x_3x_4^2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & \omega^5
 \end{array}$$

Instead of explicitly transforming the matrix into an upper-triangular matrix through row-reduction (which could easily be done by, letting **C**, **D**, **E** representing the first 6, next 6, and last 6 rows by switching **D** and **E**, and then letting **D** be replaced by **D** – **C** and **E** by **D** – **C**), the determinant can be calculated through the utilization of computing technology. The result is $\omega^{24}(\omega - 1)^{12}$, which is nonzero as long as $\omega \neq 0, 1$, which is the case if $q > 2$, which is the case, since $q > 3$. Thus, these 18 row vectors are linearly independent among themselves. Therefore, each categorization of the 35 row vectors are linearly independent within each categorization. Since the categorizations were created so that each category was independent of each other (that is, every vector in one categorization was linearly independent from all vectors in all other categorizations), each of the 35 row vectors must be linearly independent. Therefore, the upper bound is achieved, and the dimension must be 35. \square

3.6. For Sufficiently Large q , $k \geq l(j) + 1$. First, some definitions are necessary. Note that in all of the above matrices, in the rows which correspond to the monomials, for each degree of each monomial, a diagonal submatrix was formed. For example, examine the following:

$$\begin{array}{cccccc}
 & (1, 0, 0) & (0, 1, 0) & (0, 0, 1) & (\omega, 0, 0) & (0, \omega, 0) & (0, 0, \omega) \\
 x_1 & 1 & 0 & 0 & \omega & 0 & 0 \\
 x_2 & 0 & 1 & 0 & 0 & \omega & 0 \\
 x_3 & 0 & 0 & 1 & 0 & 0 & \omega \\
 x_1^2 & 1 & 0 & 0 & \omega^2 & 0 & 0 \\
 x_1^2 & 0 & 1 & 0 & 0 & \omega^2 & 0 \\
 x_3^2 & 0 & 0 & 1 & 0 & 0 & \omega^2
 \end{array}$$

In order to allow for arbitrary l to be included in the argument, consider the equivalent abbreviated matrix for this matrix (which is not contingent upon the choice of l):

$$(1) \quad (\omega) \\ \begin{matrix} x_i & 1 & \omega \\ x_i^2 & 1 & \omega^2 \end{matrix} .$$

Thus, the points are replaced by the non-zero component of each point, and each monomial is differentiated only by its degree. Hence, each entry in this abbreviated matrix corresponds to an l -by- l block of the larger matrix with the entry element along the diagonal. Note that each row vector in this l -by- l block is linearly independent, so if the determinant of this abbreviated matrix is shown to be non-zero for certain q , then each row vector in the abbreviated matrix is linearly independent from each other, implying that each l -by- l block is linearly independent from each other, thereby proving that the submatrix represented by the abbreviated matrix contains all linearly independent rows.

As a short aside, note that the first row vector of the complete matrix representation of the code (this row corresponds to the constant polynomial) is always linearly independent from the other row vectors since it is the only row vector which has a non-zero element when evaluated at the origin.

To continue with the argument based upon the determinant, examine how a determinant is calculated. An entry in the first row of the matrix is multiplied by 1 or -1 and then multiplied by the determinant of its cofactor. This process is repeated until an element from the second to last row is multiplied by 1 or -1 and then by an element in the last row which is not in the same column (which is the only element in its cofactor if, when cofactors were created in previous stages, all rows and columns removed remain removed). All of these multiplications are then added together to form the determinant. Note that in each multiplication, only one element from each column and row is used. Therefore, in order to find the highest degree of ω in the determinant, all that must be done is to find the way in which to maximize the exponent of ω in the multiplications. A sketch of an arbitrary matrix reveals that this is achieved by multiplying along the main diagonal:

$$\begin{matrix} & (1) & (\omega) & (\omega^2) & (\omega^3) & (\omega^4) & \dots \\ x_i & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \dots \\ x_i^2 & 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \dots \\ x_i^3 & 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \dots \\ x_i^4 & 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \dots \\ x_i^5 & 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{matrix} .$$

The reason that the main diagonal provides the highest degree is that if only one element from each row and column can be used in the matrix in the multiplication, then it would be desirable to have the highest degree entry in the multiplication, which is the bottom-right entry. With the removal of the rightmost and bottommost columns, the next highest degree entry is the bottom-right entry of the cofactor of the original bottom-right entry. Repeating this process yields the main diagonal. A closed formula for the maximum degree (and thus the degree of the determinant) is $\sum_{i=0}^{j-1} i(i+1) = \sum_{i=1}^{j-1} (i^2 + i) = \sum_{i=1}^{j-1} i^2 + \sum_{i=1}^{j-1} i = \frac{(j-1)(2j-1)j}{6} + \frac{(j-1)j}{2} = \frac{j(j-1)(j+1)}{3}$.

Thus, this is the degree of the determinant (a check using the Sage program: for $j = 5$, adding the exponents of each occurrence gives the degree of the determinant to be 40; the formula given above concurs). By a somewhat parallel argument, the minimum degree of the terms in

the determinant can also be found. To minimize the degree, the leftmost entry in the bottom row must be chosen; the same is true for the cofactor of this element. Continuing yields the secondary diagonal. A closed formula for the minimum degree is $\sum_1^j (j-i)i = j \sum_1^j i - \sum_1^j i^2 = j \frac{j(j+1)}{2} - \frac{j(j+1)(2j+1)}{6} = \frac{j(j-1)(j+1)}{6}$. The importance of knowing this minimum degree is that, letting the minimum degree be z , ω^z can be factored out of the determinant (in other words [letting the determinant be expressed as a polynomial with ω being considered the unknown], ω is a zero of the determinant with multiplicity z). Another check using the Sage program is that both the program and the closed formula give the degree of ω to be 20 for $j = 5$. After this factorization, the new maximum degree is $\frac{j(j-1)(j+1)}{3} - \frac{j(j-1)(j+1)}{6} = \frac{j(j-1)(j+1)}{6}$. Throwing out the ω^z term is justified in the course of proving the determinant is non-zero because for the determinant to be zero due to that term, ω would have to equal 0, which would indicate the finite field \mathbb{F}_q is of size 1 ($q = 1$), which clearly is not the case (let $q > 1$). Hence, there can be as many as $\frac{j(j-1)(j+1)}{6}$ other zeros in the determinant by an extension of the Fundamental Theorem of Algebra to finite fields. Therefore, by selecting q to fulfill $q > \frac{j(j-1)(j+1)}{6}$, there will be more elements of the finite field than zeros, so let ω be an element which is not a zero of the determinant, directly implying that the determinant is not zero. Therefore, since this abbreviated matrix represented $l(j)$ row vectors (there are j rows, each representing an l -by- l block), all $l(j)$ row vectors (plus the row vector corresponding to the constant polynomial) are linearly independent. Therefore, as long as q is sufficiently large, $k \geq l(j) + 1$. \square

```
sage: James Berg, SM450A Final Project
sage: def matrix_code_generator(j):
...     """
...     A function designed to create the abbreviated sub-matrix of
...     a matrix for the code corresponding to the coordinate hyperplane
...     arrangement. The sub-matrix corresponds exclusively to
...     polynomials consisting of one variable raised to a power.
...     The input is j, the upper bound on the polynomials used in generation.
...
...     EXAMPLES: See below for j=1,...,10
...     INPUT: j
...     OUTPUT: factored determinant of the abbreviated sub-matrix
...     """
...     w=var('w')
...     row=[0]*j
...     for k in range(j):
...         row[k]=w^k
...     CodeMatrix=[[0]*j]*j
...     for l in range(j):
...         newrow=[0]*j
...         for k in range(j):
...             newrow[k]=w^k
...         for m in range(j):
...             newrow[m]=row[m]**(l+1)
...         CodeMatrix[l]=newrow
...     CodeMatrixlist=[0]*(j**2)
...     for n in range(j):
...         for p in range(j):
...             CodeMatrixlist[n+j*p]=CodeMatrix[p][n]
...     MS=MatrixSpace(PolynomialRing(ZZ,w),j,j)
...     Code_matrix=MS.matrix(CodeMatrixlist)
...     determinant=det(Code_matrix)
...     factored_det=determinant.factor()
...     return factored_det
sage: def matrix_code_echelon(j):
...     """
...     A function designed to create the abbreviated sub-matrix
...     of a matrix for the code corresponding to the coordinate
...     hyperplane arrangement. The sub-matrix corresponds exclusively to
...     polynomials consisting of one variable raised to a power.
...     The input is j, the upper bound on the polynomials used in generation.
...
...     EXAMPLES: See below for j=1,...,5
...     INPUT: j
...     OUTPUT: echelon form of the abbreviated sub-matrix
...     """
...     w=var('w')
```

```

...     row=[0]*j
...     for k in range(j):
...         row[k]=w^k
...     CodeMatrix=[[0]*j]*j
...     for l in range(j):
...         newrow=[0]*j
...         for k in range(j):
...             newrow[k]=w^k
...         for m in range(j):
...             newrow[m]=row[m]**(l+1)
...         CodeMatrix[l]=newrow
...     CodeMatrixlist=[0]*(j**2)
...     for n in range(j):
...         for p in range(j):
...             CodeMatrixlist[n+j*p]=CodeMatrix[p][n]
...     MS=MatrixSpace(PolynomialRing(ZZ,w),j,j)
...     Code_matrix=MS.matrix(CodeMatrixlist)
...     echelon=Code_matrix.echelon_form()
...     return echelon
sage: matrix_code_generator(1)
1
sage: matrix_code_echelon(1)
[1]
sage: matrix_code_generator(2)
(w - 1) * w
sage: matrix_code_echelon(2)
[ 1  w]
[ 0 w^2 - w]
sage: matrix_code_generator(3)
(w + 1) * (w - 1)^3 * w^4
sage: matrix_code_echelon(3)
[ 1 0 0 0]
[ 0 w^2 - w w^4 - w^2 0]
[ 0 0 w^6 - w^5 - w^4 + w^3 0]
sage: matrix_code_generator(4)
(w + 1)^2 * (w - 1)^6 * w^10 * (w^2 + w + 1)
sage: matrix_code_echelon(4)
[ 1 0 0 0]
[ 0 w^2 - w w^4 - w^2 w^6 - w^5 - w^4 + w^3]
[ 0 0 w^6 - w^5 - w^4 + w^3 w^9 - w^7 - w^6 + w^4]
[ 0 0 0 w^12 - w^11 - w^10 + w^8 + w^7 - w^6]
sage: matrix_code_generator(5)
(w + 1)^4 * (w - 1)^10 * w^20 * (w^2 + 1) * (w^2 + w + 1)^2
sage: matrix_code_echelon(5)
[ 1 0 0 0]
[ 0 w^2 - w w^4 - w^2 w^6 - w^5 - w^4 + w^3 w^9 - w^7 - w^6 + w^4]
[ 0 0 w^6 - w^5 - w^4 + w^3 w^9 - w^7 - w^6 + w^4 w^12 - w^11 - w^10 + w^8 + w^7 - w^6]
[ 0 0 0 w^12 - w^11 - w^10 + w^8 + w^7 - w^6 w^16 - w^14 - w^13 - w^12 + w^11 + w^10 + w^9 - w^7]
[ 0 0 0 0 w^20 - w^19 - w^18 + 2*w^15 - w^12 - w^11 + w^10]
sage: matrix_code_generator(6)
(w + 1)^6 * (w - 1)^15 * w^35 * (w^2 + 1)^2 * (w^2 + w + 1)^3 * (w^4 + w^3 + w^2 + w + 1)
sage: matrix_code_generator(7)
(w + 1)^9 * (w - 1)^21 * w^56 * (w^2 - w + 1) * (w^2 + 1)^3 * (w^2 + w + 1)^5 * (w^4 + w^3 + w^2 + w + 1)^2
sage: matrix_code_generator(8)
(w + 1)^12 * (w - 1)^28 * w^84 * (w^2 - w + 1)^2 * (w^2 + 1)^4 * (w^2 + w + 1)^7 * (w^4 + w^3 + w^2 + w + 1)^3 * (w^6 + w^5 + w^4 + w^3 + w^2 + w + 1)
sage: matrix_code_generator(9)
(w + 1)^16 * (w - 1)^36 * w^120 * (w^2 - w + 1)^3 * (w^2 + 1)^6 *
(w^2 + w + 1)^9 * (w^4 + 1) * (w^4 + w^3 + w^2 + w + 1)^4 *
(w^6 + w^5 + w^4 + w^3 + w^2 + w + 1)^2
sage: matrix_code_generator(10)
(w + 1)^20 * (w - 1)^45 * w^165 * (w^2 - w + 1)^4 * (w^2 + 1)^8 *
(w^2 + w + 1)^12 * (w^4 + 1)^2 * (w^4 + w^3 + w^2 + w + 1)^5 *
(w^6 + w^3 + 1) * (w^6 + w^5 + w^4 + w^3 + w^2 + w + 1)^3

```