$\mathbb{F}_q$-rational points of hypersurfaces in weighted projective spaces over finite fields

Rupert Li

under the direction of

Chun Hong Lo
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
July 30, 2019

Abstract

We investigate $\mathbb{F}_q$-rational points on hypersurfaces in weighted projective spaces over the finite field $\mathbb{F}_q$. Particularly, we consider the maximum number of $\mathbb{F}_q$-rational points that can lie on a hypersurface of a given degree, weighted projective space, and finite field. In classical projective space, Serre answered this question by proving Serre's inequality. We provide conjectures generalizing Serre's inequality to weighted projective spaces and prove some partial results. We also prove which values the number of $\mathbb{F}_q$-rational points on a given hypersurface can take, and give some further conjectures about these possible values and their distributions.

1 Introduction

Vanishing points in projective m-space over finite fields $\mathbb{F}_q$ are analogous to roots of polynomials in affine space. Thus, it is natural to investigate the order of hypersurfaces, the set of vanishing points for a degree d weighted homogeneous polynomial. An intuitive approach, as described by Datta and Ghorpade [1], provides an upper bound of the number of $\mathbb{F}_q$-rational points on the hypersurface. By projecting the hypersurface $V(F)$ in m-space onto $(m-1)$-space, they bounded $|V(F)|$ by

$$|V(F)| \leq d \left|\mathbb{P}^{m-1}(\mathbb{F}_q)\right|. \tag{1}$$

Note that if $d > q$, this bound exceeds $|\mathbb{P}^m(\mathbb{F}_q)|$, and hence this bound is only interesting for $d \leq q$.

While this bound was proven, for example by Lidl and Neiderreiter [2], an example of a homogeneous polynomial of degree $d \leq q$ with exactly $d\,|\mathbb{P}^{m-1}(\mathbb{F}_q)|$ vanishing points could not be found. However, the homogeneous polynomial

$$G_d(X_0, X_1, \ldots, X_m) := (X_1 - a_1X_0)\ldots(X_1 - a_dX_0),$$

where $a_1, \ldots, a_d$ are distinct elements of $\mathbb{F}_q$ and $d \leq q$, has exactly $dq^{m-1}+|\mathbb{P}^{m-2}(\mathbb{F}_q)|$ vanishing points in $\mathbb{P}^m(\mathbb{F}_q)$. Furthermore, $G_{q+1} := X_0G_q$ also has exactly $dq^{m-1}+|\mathbb{P}^{m-2}(\mathbb{F}_q)|$ vanishing points in $\mathbb{P}^m(\mathbb{F}_q)$. For $d, m > 1$, we have $dq^{m-1}+|\mathbb{P}^{m-2}(\mathbb{F}_q)| < dp_{m-1}$. Tsfasman, possibly motivated by these observations, conjectured in the late 1980's that $dq^{m-1} + |\mathbb{P}^{m-2}(\mathbb{F}_q)|$ was the sharp upper bound for $d \leq q + 1$, or in other words,

$$|V(F)| \leq dq^{m-1} + |\mathbb{P}^{m-2}(\mathbb{F}_q)|. \tag{2}$$

Due to the existence of G_d, this statement immediately implies

$$\max_F |V(F)| = dq^{m-1} + |\mathbb{P}^{m-2}(\mathbb{F}_q)|. \tag{3}$$

This conjecture was proven in 1989 by Serre [3] in a letter to Tsfasman, and the resulting inequality (2) is thus often called Serre's inequality. An alternate proof to Serre's inequality, which uses the intersection of $V(F)$ with a hyperplane to perform induction on m, is provided by Datta and Ghorpade [1].

Aubry et al. [4] attempted to generalize Serre's inequality to weighted projective spaces, a generalization of projective space formally defined in Section 2, over finite fields. They posed the following conjecture about hypersurfaces in weighted projective space.

Conjecture 1. *(Aubry et al.) If $1 = a_0 \leq a_1 \leq a_2 \leq \cdots \leq a_m$ and $\operatorname{lcm}(a_1, a_2, \ldots, a_m)|d$, then*

$$\max_{F \in S_d[X_0, X_1, \ldots, X_m] \setminus \{0\}} |V(F)| = \min \left\{ p_m, \frac{d}{a_1} q^{m-1} + p_{m-2} \right\}, \tag{4}$$

where $S_d[X_0, X_1, \ldots, X_m]$ is the space of weighted homogeneous polynomials of degree d in $\mathbb{F}_q[X_0, X_1, \ldots, X_m]$ with respect to the weights $a_0, \ldots, a_m$.

Note that to prove Conjecture 1, one needs only to prove the result for $d \leq a_1(q+1)$, as otherwise the right hand side of Equation (4) evaluates to $p_m = |\mathbb{P}^m(\mathbb{F}_q)|$. In that case, the degree is high enough so that one can make a polynomial in only X_0 and X_1 so that for all values of X_0 and X_1, there is a factor of the polynomial that evaluates to 0.

Aubry et al. successfully proved Conjecture 1 for $m \leq 2$. We extend this result to higher dimensions by proving upper bounds and modular congruences that $|V(F)|$ satisfies for hypersurfaces in weighted projective spaces over finite fields.

In Section 2, we review the definitions of weighted homogeneous polynomials in weighted projective space over finite fields. In Section 3, we expand the results of Aubry et al. [4] of the $m \leq 2$ case to prove specific cases of Conjecture 1 for all dimensions m. In Section 4, we investigate what specific values $|V(F)|$ can take. We prove that under certain simple conditions, $|V(F)| \equiv 1 \pmod{p}$, where p is the characteristic of $\mathbb{F}_q$, and conjecture that $|V(F)| \equiv 1 \pmod{q}$. In Section 5, we also give some empirical data and observations of the distribution of $|V(F)|$ values that support this conjecture. Finally, in Section 6 we discuss some applications of weighted projective space to error correcting code theory.

2 Preliminaries

Let k be a fixed field. Affine m-space $\mathbb{A}^m(k)$ is the set of m-tuples of elements of k. It is denoted as $\mathbb{A}^m$ for simplicity. Each of these m-tuples is called a *point* in affine space, with the individual elements of the m-tuple often called the point's *coordinates*. Let q denote a prime power and let $\mathbb{F}_q$ denote the finite field with q elements. When $k = \mathbb{F}_q$, we have $\mathbb{A}^m = \mathbb{F}_q^m$.

Projective m-space $\mathbb{P}^m$ is defined by

$$\mathbb{P}^m = \left(\mathbb{A}^{m+1} \setminus \{\mathbf{0}\}\right) / \sim,$$

where $\sim$ is defined by $(x_0, \ldots, x_m) \sim (y_0, \ldots, y_m)$ if there exists $\lambda \in \mathbb{F}_q^*$ such that for all $i \in \{0, \ldots, m\}$, we have $y_i = \lambda x_i$.

For any integer n, define p_n as

$$p_n = \begin{cases} q^n + q^{n-1} + \cdots + 1 & \text{for } n \geq 0 \\ 0 & \text{for } n < 0. \end{cases}$$

Note that $p_n = |\mathbb{P}^n(\mathbb{F}_q)|$ for $n \geq 0$.

For any nonzero homogeneous degree d polynomial $F \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]$, the *projective hypersurface* $V(F)$ is the set of vanishing points, defined by

$$V(F) := \{P \in \mathbb{P}^m(\mathbb{F}_q) : F(P) = 0\}.$$

Similarly, for any nonzero polynomial $F \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]$, the *hypersurface* $Z(F)$ is the set of zeroes, defined by

$$Z(F) := \left\{P \in \mathbb{A}^{m+1} : F(P) = 0\right\}.$$

Weighted projective space over a finite field, a generalization of projective space, is defined by

$$\mathbb{P}(a_0, a_1, \ldots, a_m) = \left(\overline{\mathbb{F}}_q^{m+1} \setminus \{\mathbf{0}\}\right) / \sim,$$

where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$, the weights $a_0, a_1, \ldots, a_m$ are positive integers, and $\sim$ is defined by $(x_0, \ldots, x_m) \sim (y_0, \ldots, y_m)$ if there exists $\lambda \in \overline{\mathbb{F}}_q^*$ such that $y_i = \lambda^{a_i} x_i$ for all $i \in \{0, \ldots, m\}$. Notice that $\mathbb{P}(1, 1, \ldots, 1) = \mathbb{P}^m(\mathbb{F}_q)$.

The corresponding equivalence class under the equivalence relation $\sim$ is called a *weighted projective point* and denoted by $(x_0 : x_1 : \cdots : x_m)$. A weighted projective point is said to be $\mathbb{F}_q$-rational if $(x_0^q : x_1^q : \cdots : x_m^q) = (x_0 : x_1 : \cdots : x_m)$. Hilbert's theorem 90 can be used to show that every $\mathbb{F}_q$-rational point has at least one representative in $\mathbb{F}_q^{m+1} \setminus \{\mathbf{0}\}$. Reid [5] further showed that each $\mathbb{F}_q$-rational point has exactly $q-1$ such representatives. Furthermore, the total number of $\mathbb{F}_q$-rational points is p_m, the same as in the unweighted case.

The definition of homogeneity for a hypersurface of degree d must be generalized so that a nonzero polynomial $F \in \mathbb{F}_q[X_0, X_1, \ldots, X_m]$ is homogeneous of degree d if every term has degree d when we measure X_i with weight a_i, so that

$$F\left(\lambda^{a_0} X_0, \lambda^{a_1} X_1, \ldots, \lambda^{a_m} X_m\right) = \lambda^d F\left(X_0, X_1, \ldots, X_m\right)$$

for all $\lambda \in \overline{\mathbb{F}}_q^*$. This ensures that the notion of vanishing points is well-defined over the different representatives of a weighted projective point.

The space of weighted homogeneous polynomials of degree d in the weighted projective space $\mathbb{P}(a_0, \ldots, a_m)$ over $\mathbb{F}_q$ with variables $X_0, \ldots, X_m$ is denoted by

$$S_d[X_0, \ldots, X_m] \subset \mathbb{F}_q[X_0, \ldots, X_m].$$

By rescaling the weights, we have that for any positive integer b,

$$\mathbb{P}(a_0 b, \ldots, a_m b) \cong \mathbb{P}(a_0, \ldots, a_m).$$

Delorme [6] showed that for any index i and any positive integer b coprime to a_i, the weight reduction

$$\mathbb{P}(a_0b, \ldots, a_{i-1}b, a_i, a_{i+1}b, \ldots, a_mb) \cong \mathbb{P}(a_0, a_1, \ldots, a_m)$$

holds. In particular, the Delorme weight reduction respects Conjecture 1 in the sense that for a fixed q value, there exists a bijection between the hypersurfaces for degree db with weights $1, a_1b, \ldots, a_mb$ and the hypersurfaces for degree d with weights $1, a_1, \ldots, a_m$ that respects the number of vanishing points of the hypersurfaces.

Hence, in the statement of Conjecture 1 we may assume $\gcd(a_1, a_2, \ldots, a_m) = 1$. This allowed Aubry et al. to assume that a_1 and a_2 are coprime in their proof of the $m = 2$ case for Conjecture 1.

3 Hypersurfaces in $\mathbb{P}(1, \ldots, 1, a_{m-1}, a_m)$

We generalize the proof of Conjecture 1 for $m \leq 2$ by Aubry et al. [4, Theorem 1] to higher-dimensional weighted projective spaces by the following theorem.

Theorem 1. *Let $F \in S_d[X_0, X_1, \ldots, X_m]$ be a weighted homogeneous polynomial where the weights satisfy $a_0, \ldots, a_{m-2} = 1$ and $\mathrm{lcm}(a_{m-1}, a_m)|d$. If there exists a hyperplane H given by $\sum_{i=0}^{m-2} c_iX_i = 0$ where $c_0, \ldots, c_{m-2} \in \mathbb{F}_q$ and at least one of them is nonzero, so that $|V(F) \cap H| = 0$, then*

$$|V(F)| \leq \min\left\{p_m, \frac{d}{a_1}q^{m-1} + p_{m-2}\right\}. \tag{5}$$

Note that for $m \geq 3$ we have $a_1 = 1$.

We first give an example of the theorem, describe the assumptions that can be made for the proof of the theorem, and provide some background notations and results before we prove the theorem.

An example of the hyperplane intersection criterion is in $\mathbb{P}(1, 1, 2)$ over $\mathbb{F}_5 \cong \mathbb{Z}/5\mathbb{Z}$. The weighted homogeneous polynomial $F : X_0^4 + 2X_1^4 + X_1^2X_2 + X_2^2$ has projective hypersurface $V(F) = \{(1{:}0{:}2), (1{:}0{:}3), (1{:}1{:}1), (1{:}1{:}3), (1{:}2{:}2), (1{:}2{:}4), (1{:}3{:}2), (1{:}3{:}4), (1{:}4{:}1), (1{:}4{:}3)\}$. If hyperplane H is defined by $X_0 = 0$, then we see that $|V(F) \cap H| = 0$. Furthermore, as $m = 2$, we have that $a_0 = 1$, as well as $\mathrm{lcm}(a_1, a_2) = 2|d$, where $d = 4$. Hence, this polynomial is an example of a weighted homogeneous polynomial that satisfies the criteria for Theorem 1.

To prove Theorem 1, we assume without loss of generality that $a_{m-1} \leq a_m$. From the result by Aubry et al. [4, Theorem 1], we may assume $m \geq 3$. Let $F \in S_d[X_0, \ldots, X_m]$ be a nonzero polynomial that satisfies the constraints of Theorem 1. As Aubry et al. [4, Remark 3] demonstrated, under an $\mathbb{F}_q$-rational change of variables that respects the grading, H can be transformed into $X_0 = 0$. Hence we assume that H is defined by $X_0 = 0$. Assuming that $d < a_1(q+1) = q+1$, we are tasked with showing

$$|V(F)| \leq \frac{d}{a_1} q^{m-1} + p_{m-2} = dq^{m-1} + p_{m-2}. \tag{6}$$

We do this by following the method of Aubry et al. [4]. First, note that having $a_0 = 1$ allows for every point $(x_0 : x_1 : \cdots : x_m)$ for which $x_0 \neq 0$ to have a unique representation with $(1 : x'_1 : \cdots : x'_m)$, where $x'_i = x_i / x_0^{a_i}$. Furthermore, the point is $\mathbb{F}_q$-rational if and only if $x'_1, \ldots, x'_m \in \mathbb{F}_q$. Hence the embedding

$$\mathbb{A}^m \hookrightarrow \mathbb{P}(1, \ldots, 1, a_{m-1}, a_m) : (x'_1, \ldots, x'_m) \mapsto (1 : x'_1 : \cdots : x'_m)$$

identifies $\mathbb{A}^m$ with the subset of $\mathbb{P}(1, \ldots, 1, a_{m-1}, a_m)$ where $X_0 \neq 0$, in a manner that continues to hold if one restricts to $\mathbb{F}_q$-rational points. We use the notation of Aubry et al. [4] of the hyperplane at infinity $H_\infty : X_0 = 0$.

The zeros of F in $\mathbb{A}^m$ are the zeros of the dehomogenized polynomial $F(1, x'_1, \ldots, x'_m)$. Conversely, there is a natural way of homogenizing a polynomial over variables $x'_1, \ldots, x'_m$ by substituting X_i as x'_i, and adding as many X_0 factors to each term as minimally needed. We generalize the notion of lines in $\mathbb{P}(1, a_1, a_2)$ as defined by Aubry et. al. [4] to hyperplanes represented by either a homogenized linear equation, or the hyperplane at infinity.

Definition 1. An *$\mathbb{F}_q$-rational hyperplane*, or simply a hyperplane, in $\mathbb{P}(1, a_1, a_2, \ldots, a_m)$ is a subset defined by an equation given by one of the following types.

- Type 0: $H_\infty : X_0 = 0$.
- Type 1: Lines of the form $c_0 X_0^{a_1} + X_1 = 0$ with $c_0 \in \mathbb{F}_q$.
- Types $2 \leq i \leq m$: Lines of the form

$$c_0 X_0^{a_m} + \sum_{j=1}^{i-1} c_j X_j X_0^{a_i - a_j} + X_i = 0$$

with $c_i \in \mathbb{F}_q$ for all $i \in \{0, \ldots, m-1\}$.

As Aubry et al. [4, Remark 3] demonstrated, each hyperplane of type i, under an $\mathbb{F}_q$-rational change of variables that respects the grading, can be transformed into $X_i = 0$.

To prove Theorem 1, we need the following lemmas about hyperplane intersections.

Lemma 1. *Any hyperplane in $\mathbb{P}(1, a_1, a_2, \ldots, a_m)$ contains exactly p_{m-1} rational points, and any pair of distinct $\mathbb{F}_q$-rational hyperplanes in $\mathbb{P}(1, a_1, a_2, \ldots, a_m)$ has at least p_{m-2} rational points in common.*

Proof. Use an $\mathbb{F}_q$-rational change of variables that respects the grading to transform a hyperplane into the form $X_i = 0$, where the hyperplane is of type i. From there, the number of rational points on the hyperplane is equal to $|\mathbb{P}^{m-1}(\mathbb{F}_q)| = p_{m-1}$.

With a pair of hyperplanes, transform the hyperplanes so that one is of the form $X_i = 0$. The other hyperplane, say of type j, where without loss of generality $i \leq j$, is of the form

$$\sum_{k=0}^{j-1} c_k X_k X_0^{a_j - a_k} + X_j = 0$$

where all the c_k are fixed.

If $i = j$, this becomes $\sum\limits_{k=0}^{j-1} c_k X_k X_0^{a_j - a_k} = 0$, which yields p_{m-2} solutions when $X_0 = 0$, so in this case there are at least p_{m-2} rational points in common.

If $i < j$, by combining the two equations, a point is on both the hyperplanes if and only if it satisfies the equation

$$\sum_{k=0}^{i-1} c_k X_k X_0^{a_j - a_k} + \sum_{k=i+1}^{j-1} c_k X_k X_0^{a_j - a_k} + X_j = 0.$$

A point satisfies this equation if and only if

$$X_j = -\left(\sum_{k=0}^{i-1} c_k X_k X_0^{a_j - a_k} + \sum_{k=i+1}^{j-1} c_k X_k X_0^{a_j - a_k} \right),$$

which yields $q^{m-1} - 1$ choices from the $m - 1$ choices for $X_0, \ldots, X_{j-1}, X_{j+1}, \ldots, X_m$ except when all coordinates are 0. However, as the equation is still homogeneous and we have not distinguished points up to scaling, we must divide by $q - 1$ to yield p_{m-2} points on the intersection of two distinct $\mathbb{F}_q$-rational hyperplanes. ■

Lemma 2. *There are at least p_{m-2} hyperplanes through two given distinct affine rational points, i.e. two points where $X_0 \neq 0$.*

Proof. Express the two affine rational points as $(1{:}x_1{:}\cdots{:}x_m)$ and $(1{:}y_1{:}\cdots{:}y_m)$. We count how many hyperplanes of type i for $1 \leq i \leq m$ pass through both the two affine rational points.

We solve for the possible values of c_i, which must be solutions to the system of equations

$$\begin{cases} c_0 + \sum_{j=1}^{i-1} c_j x_j + x_i &= 0 \\ c_0 + \sum_{j=1}^{i-1} c_j y_j + y_i &= 0. \end{cases}$$

As long as $c_0 = -x_i - \sum_{j=1}^{i-1} c_j x_j$, the first equation is satisfied, and thus the second becomes

$$y_i - x_i + \sum_{j=1}^{i-1} c_j(y_j - x_j) = 0.$$

If $x_j = y_j$ for all $j \in \{1, 2, \dots, i-1\}$, then there are q choices for each c_j, resulting in q^{i-1} hyperplanes through the two affine rational points.

Otherwise, there exists some value $j \in \{1, 2, \dots, i-1\}$ such that $y_j \neq x_j$. If there is such a j with $j < i$, then c_j is uniquely defined by the other c_k, x_k, and y_k. Other than that, there are no restrictions, so there are q choices each for the values of the $i-2$ other c_k where $k \notin \{0, j\}$. This yields q^{i-2} hyperplanes through two affine rational points.

At minimum, there are q^{i-2} hyperplanes of type i through two affine rational points, meaning that summing over all types i, there are at least $1 + q + \cdots + q^{m-2} = p_{m-2}$ number of $\mathbb{F}_q$-rational hyperplanes through two distinct affine rational points. ■

We are now ready to prove the upper bound for $|V(F)|$ stated in Equation (6).

Proof of Theorem 1. We prove the result by induction on m. The cases $m \leq 2$ have been proven by Aubry et al. [4, Theorem 1], so we assume in the inductive step that $m \geq 3$.

Let $H_1, \dots, H_t$ be the distinct hyperplane factors of F, each of the types defined in Definition 1. For each integer $1 \leq i \leq t$, define $L_i = V(H_i)$, and similarly let $L_\infty = V(H_\infty)$. Define L by

$$L = \bigcup_{i=1}^{t} L_i.$$

There are p_{m-2} total hyperplanes, the hyperplanes of type 0 through $m-2$, inclusive, that have degree 1. For $m \geq 3$, we have $p_{m-2} \geq q+1$, so as $d \leq q+1$, we have $d \geq t$ as each hyperplane has degree at least 1.

The first part of the proof is to show that $|L| \leq t(q^{m-1}) + p_{m-2}$. We proceed by induction on t. The case $t = 0$ is trivial, and the case $t = 1$ follows from Lemma 1. For the inductive step, we have

$$\begin{aligned} |L| &= \left| \bigcup_{i=1}^{t} L_i \right| \\ &= \left| \bigcup_{i=1}^{t-1} L_i \right| + |L_t| - \left| \bigcup_{i=1}^{t-1} L_i \cap L_t \right| \\ &\leq (t-1)(p_{m-1} - p_{m-2}) + p_{m-2} + p_{m-1} - p_{m-2}, \end{aligned}$$

where the inequality uses Lemma 1. This reduces to

$$\begin{aligned} (t-1)(p_{m-1} - p_{m-2}) + p_{m-2} + p_{m-1} - p_{m-2} &= t(p_{m-1} - p_{m-2}) + p_{m-2} \\ &= tq^{m-1} + p_{m-2}. \end{aligned}$$

We proceed with three cases.

Case 1: Suppose that $V(F) \setminus L \subseteq L_\infty \setminus \{L'_\infty\}$, where L'_∞ is the space with $X_0 = X_1 = 0$.

1. If there exists i such that $L_i = L_\infty$, then $V(F) = L$, so

   $$|V(F)| = |L| \leq tq^{m-1} + p_{m-2} \leq dq^{m-1} + p_{m-2}$$

   by the previous observation.

2. Otherwise, $L_i \neq L_\infty$ for all i. We consider two cases for whether t equals d or not.

   - If $t = d$, then all H_i's are of types 0 through $m-2$, inclusive, and $V(F) = L$ as F completely factors by the H_i's, so again the bound follows.
   - Otherwise, $t < d$, in which case

     $$\begin{aligned} |V(F)| &\leq |L| + |L_\infty \setminus \{L'_\infty\}| \\ &= |L| + p_{m-1} - p_{m-2} \\ &\leq tq^{m-1} + p_{m-2} + q^{m-1} \\ &= (t+1)q^{m-1} + p_{m-2} \\ &\leq dq^{m-1} + p_{m-2}. \end{aligned}$$

Case 2: There exists a point $P \in \mathbb{A}^m$ that lies in $V(F) \setminus L$. Let X denote the set of pairs (P', H) of $\mathbb{F}_q$-rational points and $\mathbb{F}_q$-rational hyperplanes such that $P, P' \in V(F) \cap H$

and $P \neq P'$. We create upper and lower bounds of $|X|$. First,

$$\begin{aligned}|X| &= \sum_{P' \in V(F) \setminus \{P\}} |\{H : H \text{ is a hyperplane with } P, P' \in H\}| \\ &\geq \sum_{P' \in V(F)^{\mathrm{aff}} \setminus \{P\}} p_{m-2} \\ &= \left|V(F)^{\mathrm{aff}} \setminus \{P\}\right| p_{m-2},\end{aligned}$$

where the inequality results from Lemma 2 and $V(F)^{\mathrm{aff}} = V(F) \cap \mathbb{A}^m = V(F) \setminus L_\infty$. On the other hand, we have

$$|X| = \sum_{i=1}^{m} \sum_{\substack{H \ni P \\ H \text{ type } i}} (|V(F) \cap H| - 1).$$

Using the change of variables as defined by Aubry et al. [4, Remark 3], we view each type i hyperplane as defined by $X_i = 0$. This reduces the summand to the number of $\mathbb{F}_q$-rational vanishing points of $F(X_0, \ldots, X_{i-1}, 0, X_{i+1}, \ldots, X_m)$ in $\mathbb{P}(a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_m)$. By the inductive hypothesis, $V(F) \cap H$ has at most $\frac{d}{a_1} q^{m-2} + p_{m-3}$ zeroes if $i > 1$ and at most $\frac{d}{a_2} q^{m-2} + p_{m-3}$ vanishing points if $i \leq 1$. Either way, it has at most $dq^{m-2} + p_{m-3}$ vanishing points.

There are q^{i-1} hyperplanes of type i that pass through P out of the q^i total hyperplanes of type i. Hence,

$$\begin{aligned}|X| &= \sum_{i=1}^{m} \sum_{\substack{H \ni P \\ H \text{ type } i}} (|V(F) \cap H| - 1) \\ &\leq \sum_{i=1}^{m} q^{i-1} \left(dq^{m-2} + p_{m-3} - 1\right) \\ &= p_{m-1} \left(dq^{m-2} + p_{m-3} - 1\right) \\ &= qp_{m-1} \left(dq^{m-3} + p_{m-4}\right).\end{aligned}$$

Combining the two bounds on $|X|$ yields

$$\left|V(F)^{\mathrm{aff}} \setminus \{P\}\right| p_{m-2} \leq |X| \leq qp_{m-1} \left(dq^{m-3} + p_{m-4}\right).$$

This allows us to bound $\left|V(F)^{\text{aff}}\right|$ by

$$\begin{aligned}\left|V(F)^{\text{aff}}\right| &\leq \frac{qp_{m-1}}{p_{m-2}}\left(dq^{m-3}+p_{m-4}\right)+1\\ &= \left(q^2+\frac{q}{p_{m-2}}\right)\left(dq^{m-3}+p_{m-4}\right)+1\\ &= dq^{m-1}+q^2p_{m-4}+\frac{qp_{m-4}+dq^{m-2}}{p_{m-2}}+1.\end{aligned}$$

Using the fact that $d < q+1$, or equivalently $d \leq q$, this simplifies to

$$\begin{aligned}\left|V(F)^{\text{aff}}\right| &\leq dq^{m-1}+p_{m-2}-q+\frac{qp_{m-4}+q^{m-1}}{p_{m-2}}\\ &= dq^{m-1}+p_{m-2}+q\left(\frac{p_{m-4}+q^{m-2}-p_{m-2}}{p_{m-2}}\right)\\ &= dq^{m-1}+p_{m-2}-q\left(\frac{q^{m-3}}{p_{m-2}}\right). \qquad (7)\end{aligned}$$

To bound $|V(F)|$, we add $|V(F)\cap H_\infty|=0$ into Inequality (7), resulting in

$$\begin{aligned}|V(F)| &\leq dq^{m-1}+p_{m-2}-q\left(\frac{q^{m-3}}{p_{m-2}}\right)+|V(F)\cap H_\infty|\\ &\leq dq^{m-1}+p_{m-2},\end{aligned}$$

as desired. This ends the proof for Case 2.

Case 3: There exists a point $P \in L'_\infty$ that lies in $V(F)\setminus L$.

As H is defined by $X_0=0$ and $|V(F)\cap H|=0$, there is no element of $L'_\infty \subset L_\infty$ that is in $V(F)$. Hence, the proof is complete. ■

Remark 1. Case 1 of the proof does not rely on any of the assumptions made specifically in Theorem 1, and instead works in full generality under the conditions of Conjecture 1. Thus, it could be used in a proof of Conjecture 1, though case 2 of the proof of Theorem 1 is not strong enough for the generality of Conjecture 1.

Remark 2. If we do not assume the $|V(F)\cap H|=0$ condition in Theorem 1, a nontrivial bound can still be reached for $m=3$, and a bound for any dimension can be created inductively. However, the inequalities in Case 2 involve additional terms for each type of hyperplane. This bound is worse than the bound in Conjecture 1. In addition, case 3 becomes nontrivial, requiring a generalization of case 3 of the proof by Aubry et al. [4, Theorem 1].

Removing the requirements in Theorem 1 of having $a_0 = 1$ and $\operatorname{lcm}(a_{m-1}, a_m)|d$ makes Inequality (5) no longer hold. However, when $m = 1$, the following theorem provides an upper bound for $|V(F)|$ without any requirements on the hypersurface other than $\gcd(a_0, a_1) = 1$, which can always be achieved through the Delorme weight reduction.

Theorem 2. *Let $F \in S_d[X_0, X_1]$ be a weighted homogeneous polynomial in $\mathbb{P}(a_0, a_1)$ where $\gcd(a_0, a_1) = 1$. Then*

$$|V(F)| \leq \begin{cases} \min\left(q+1, \frac{d}{a_0a_1}\right) & \text{if } a_0a_1|d, \\ \min\left(q+1, \left\lceil \frac{d}{a_0a_1} \right\rceil + 1\right) & \text{otherwise.} \end{cases} \tag{8}$$

Proof. Similar to Theorem 1, we need only to prove the nontrivial bound.

If $a_0a_1|d$, then the result follows from Aubry et al. [4, Example 1]. So we assume $a_0a_1 \nmid d$.

Let $d = qa_0a_1 + r$, where $q, r \in \mathbb{N}$ and $0 < r < a_0a_1$. Then $\left\lceil \frac{d}{a_0a_1} \right\rceil + 1 = q + 2$. It suffices to show that $|V(F)| \leq q + 2$. We claim that F has a monomial factor of weighted degree of either r or $r + a_0a_1$.

As $r < a_0a_1$, there is at most one solution to the Diophantine equation $xa_0 + ya_1 = r$ in x and y where $0 \leq x$ and $0 \leq y$. Note that we may restrict $x < a_1$ and $y < a_0$ without losing any solutions. If such a solution exists, say $(x, y) = (x_0, y_0)$, where $0 \leq x_0 < a_1$ and $0 \leq y_0 < a_0$, there are exactly two solutions to the Diophantine equation $xa_0 + ya_1 = r + a_0a_1$ in x and y where $0 \leq x$ and $0 \leq y$, $(x, y) = (x_0 + a_1, y_0), (x_0, y_0 + a_0)$, but none of these solutions have $x < a_1$ and $y < a_0$. Moreover, the converse of this statement is true. Hence, as there are either one or two solutions to the Diophantine equation $xa_0 + ya_1 = r + a_0a_1$ in x and y where $0 \leq x$ and $0 \leq y$, if there is no such solution to $xa_0 + ya_1 = r$, then there is exactly one solution to the Diophantine equation $xa_0 + ya_1 = r + a_0a_1$.

To conclude, there is exactly one integer solution to $xa_0 + ya_1 \in \{r, r + a_0a_1\}$ within the bounds $0 \leq x < a_1$ and $0 \leq y < a_0$. Say this solution is $(x, y) = (e_0, e_1)$. We show that every monomial in F has $X_0^{e_0}X_1^{e_1}$ as a factor.

Any monomial of F must be of the form $cX_0^{d_0}X_1^{d_1}$, where $d_0a_0 + d_1a_1 = d$. Define nonnegative integers q_0, q_1, $r_0 < a_1$, and $r_1 < a_0$ so that $d_0 = q_0a_1 + r_0$ and $d_1 = q_1a_0 + r_1$. This gives us $r_0a_0 + r_1a_1 = (q - q_0 - q_1)a_0a_1 + r$, but also $r_0a_0 + r_1a_1 < 2a_0a_1$, so $q - q_0 - q_1 \in \{0, 1\}$. By our analysis of this Diophantine equation, this means $(r_0, r_1) = (e_0, e_1)$, and thus every monomial in F has $X_0^{e_0}X_1^{e_1}$ as a factor.

Hence, F has a monomial factor of weighted degree of either r or $r + a_0a_1$. This factor gives us two solutions: (1:0) and (0:1). The remaining polynomial $F' = FX_0^{-e_0}X_1^{-e_1}$ has degree $d' \in \{(q-1)a_0a_1, qa_0a_1\}$. As $a_0a_1|d'$, we use the result of Aubry et al. [4, Example 1] that such a weighted homogeneous polynomial has $|V(F')| \leq \frac{d'}{a_0a_1} \in \{q-1, q\}$. F' can thus contribute at most q solutions to F. Combining the two solutions from the $X_0^{e_0}X_1^{e_1}$ factor with the at most q solutions from $F' = FX_0^{-e_0}X_1^{-e_1}$ gives us $|V(F)| \leq q+2$, and the proof is thus complete. ■

Remark 3. If $a_0 = 1$, this bound can be reduced to $\min\left\{q+1, \left\lceil \frac{d}{a_1} \right\rceil\right\}$ as the common factor of weighted degree $r < a_1$ cannot have an X_1 term.

Remark 4. The $\gcd(a_0, a_1) = 1$ condition can be removed from Theorem 2. This means that the possible degrees d will all be multiples of $\gcd(a_0, a_1)$, and the $a_0a_1|d$ case instead becomes $\operatorname{lcm}(a_0, a_1)|d$. For values of d that do not satisfy $\gcd(a_0, a_1)|d$, the inequality is trivially true as there is no such weighted homogeneous polynomial F.

Slightly modifying the same technique as in the proof by Aubry et al. [4, Theorem 1], but using the result in Theorem 2, along with Remark 3 and Remark 4, the following corollary addresses the $\mathbb{P}(1, a_1, a_2)$ case without the divisibility requirement of Theorem 1.

Corollary 3. *Let $F \in S_d[X_0, X_1, X_2]$ be a weighted homogeneous polynomial where $a_0 = 1$ and $a_1 \leq a_2$. Then*

$$|V(F)| \leq \min\left(q^2+q+1, \left\lceil \frac{d}{a_1} \right\rceil q+2\right).$$

4 $\mathbb{F}_q$-rational Points of Hypersurfaces in Weighted Projective Space

After computing values of $|V(F)|$ for all polynomials in a fixed weighted projective space, finite field, and degree, only specific values of $|V(F)|$ were observed. As a result of these observations, we pose the following conjecture.

Conjecture 2. *Let $F \in S_d[x_0, \ldots, x_m]$ be a weighted homogeneous polynomial in $\mathbb{P}(a_0, \ldots, a_m)$ over $\mathbb{F}_q$, where $d \leq m$. Then $|V(F)| \equiv 1 \pmod{q}$.*

In addition to empirical evidence supporting Conjecture 2, the following theorem, a weaker statement of the conjecture, was proven.

Theorem 4. *Let $F \in S_d[x_0, \ldots, x_m]$ be a weighted homogeneous polynomial in $\mathbb{P}(a_0, \ldots, a_m)$ over $\mathbb{F}_q$, where $d \leq m$. Let p denote the characteristic of $\mathbb{F}_q$. Then $|V(F)| \equiv 1 \pmod{p}$.*

The proof of the theorem is a slight modification of the proof of the Chevalley-Warning Theorem by Serre [7, Theorem 3]. To prove the theorem, we need the following two lemmas, the former of which is a result by Serre [7, p. 5].

Lemma 3 (Serre)**.** *For integer $n \geq 0$,*

$$\sum_{x \in \mathbb{F}_q} x^n = \begin{cases} -1 & \textit{for } n > 0, (q-1) \mid n \\ 0 & \textit{otherwise,} \end{cases}$$

where $x^0 = 1$ even if $x = 0$.

Lemma 4. *Let $F \in S_d[x_0, \dots, x_m]$ be a weighted homogeneous polynomial in $\mathbb{P}(a_0, \dots, a_m)$ over $\mathbb{F}_q$, where $d \leq m$. Let p denote the characteristic of $\mathbb{F}_q$. Then $|Z(F)| \equiv 0 \pmod{p}$.*

Proof. For $\vec{x} = (x_0, \dots, x_m) \in \mathbb{A}^{m+1}$, define $G(\vec{x}) = 1 - F(\vec{x})^{q-1}$. For a fixed $\vec{x}$, note that $G(\vec{x}) \in \mathbb{F}_q$. If $\vec{x} \in Z(F)$, then $G(\vec{x}) = 1$; otherwise, $G(\vec{x}) = 0$. Thus,

$$|Z(F)| \equiv \sum_{\vec{x}} G(\vec{x}) \pmod{p}.$$

For vectors $\vec{d} \in \mathbb{N}^{m+1}$ where $\sum_i a_i d_i = d(q-1)$, define $c_{\vec{d}} \in \mathbb{F}_q$ such that

$$F(\vec{x})^{q-1} = \sum_{\vec{d}} c_{\vec{d}} x_0^{d_0} \cdots x_m^{d_m}.$$

As $\displaystyle\sum_i a_i d_i = d(q-1) < (m+1)(q-1)$, by the Pigeonhole Principle, there exists j such that $a_j d_j < q-1$, or in other words $d_j \leq \frac{q-2}{a_j} \leq q-2$. Hence,

$$\sum_{\vec{x} \in \mathbb{A}^{m+1}} x_0^{d_0} \cdots x_m^{d_m} = \sum_{x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_m \in \mathbb{F}_q} \left(x_0^{d_0} \cdots x_{j-1}^{d_{j-1}} x_{j+1}^{d_{j+1}} \cdots x_m^{d_m} \sum_{x_j \in \mathbb{F}_q} x_j^{d_j} \right).$$

By Lemma 3, the internal sum is zero, and so the entire sum evaluates to 0. Now,

$$\begin{aligned} \sum_{\vec{x} \in \mathbb{A}^{m+1}} G(\vec{x}) &= q^{m+1} - \sum_{\vec{x} \in \mathbb{A}^{m+1}} F(\vec{x})^{q-1} \\ &= - \sum_{\vec{x} \in \mathbb{A}^{m+1}} \sum_{\vec{d}} c_{\vec{d}} x_0^{d_0} \cdots x_m^{d_m} = - \sum_{\vec{d}} \left(c_{\vec{d}} \sum_{\vec{x} \in \mathbb{A}^{m+1}} x_0^{d_0} \cdots x_m^{d_m} \right) = 0 \end{aligned}$$

where the final step results from the observation that $\displaystyle\sum_{\vec{x} \in \mathbb{A}^{m+1}} x_0^{d_0} \cdots x_m^{d_m} = 0$.

Hence, $|Z(F)| \equiv 0 \pmod{p}$. ■

We are now ready to prove Theorem 4.

Proof of Theorem 4. By Lemma 4, in $\mathbb{A}^{m+1}$ there are $|Z(F)| \equiv 0 \pmod{p}$ roots to F. As $\vec{0}$ is a trivial root of F in $\mathbb{A}^{m+1}$, there are $|Z(F)| - 1 \equiv -1 \pmod{p}$ roots to F in $\mathbb{A}^{m+1} \setminus \{\vec{0}\}$. Thus,

$$|V(F)| \equiv -1(q-1)^{-1} \equiv 1 \pmod{p},$$

as each point in $\mathbb{P}(a_0, \dots, a_m)$ has $q-1$ representatives in $\mathbb{A}^{m+1} \setminus \{\vec{0}\}$. ■

Remark 5. Applying the Delorme weight reduction when $\gcd(a_1, \dots, a_m) > 1$ allows the degree d to decrease by a factor of b while decreasing $a_1, \dots, a_m$ by a factor of b as well; however, this does not change m, and thus it may be possible to reduce d to a value of at most m, allowing Theorem 4 to apply to the hypersurface.

5 Distribution of $|V(F)|$ in Weighted Projective Space

Through a computer search that iterates over all degree d polynomials in a given weighted projective space $\mathbb{P}(a_0, \dots, a_m)$ over $\mathbb{F}_q$, the distribution of $|V(F)|$ for all the polynomials was calculated. The data is collated into Table 1, Appendix A.

Figure 1 shows a histogram of the values of $|V(F)|$ and the number of polynomials F that have each number of vanishing points for $q = d = 2$ and $\vec{a} = (1, 1, 1, 1, 2)$.

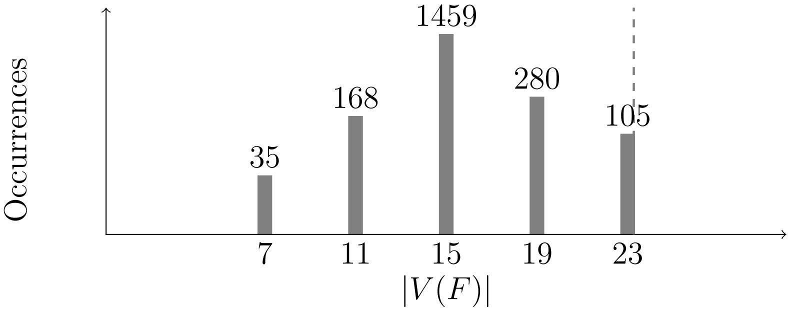

Figure 1: Distribution of $|V(F)|$ for $q = d = 2$ and $\vec{a} = (1, 1, 1, 1, 2)$.

This data supports Conjecture 2. It also supports Conjecture 1: the dashed line indicates the nontrivial bound in Equation (4).

The data in Table 1 also illustrates that if there is a weight, say without loss of generality it is a_m, such that $a_m > d$, X_m will never appear in any weighted homogeneous polynomial in that weighted projective space for degree d. Because of this, there exists a natural bijection between these weighted homogeneous polynomials and those of degree d in $\mathbb{P}(a_0. \dots, a_{m-1})$

over the same finite field. If a weighted homogeneous polynomial F in $\mathbb{P}(a_0.\dots,a_{m-1})$ has x vanishing points, then that same weighted homogeneous polynomial in $\mathbb{P}(a_0.\dots,a_m)$ has $qx+1$ vanishing points. This is because each of the x vanishing points in $(m-1)$-space makes the polynomial in m-space vanish, but there are q choices for X_m. The final solution is the trivial solution where $X_0,\dots,X_{m-1}=0$ and $X_m \neq 0$.

The distribution typically has an increasing and then decreasing pattern, though in certain cases, for example $q=3$, $d=4$, $\vec{a}=(1,1,2)$, there are additional turning points, as in occasionally the distribution is not monotonically increasing and then monotonically decreasing. In addition, quite often the most common value of $|V(F)|$ is p_{m-1}, but again this is not always the case: $q=3$, $d=2$, $\vec{a}=(1,1)$ is an example.

6 Applications to Coding Theory

In 1950, American mathematician Richard Hamming [8] invented the first error-correcting code, the Hamming (7,4) code. An error correcting code is used for resolving errors in data over noisy communication channels where the receiver may erroneously receive incorrect information. Essentially, the sender encodes the message with redundancy, following a pattern dictated by the error correcting code. This redundancy allows the receiver to handle a number of errors anywhere in the message and often correct them without need for retransmission. Hence, error correcting codes are incredibly useful and often implemented in situations where reverse channels to request retransmission are either expensive, impossible, or otherwise impractical, such as with deep space communication where messages can take hours or days to reach their desired target, or when broadcasting information to multiple sources via multicast.

Reed-Muller codes are error-correcting codes based in finite field theory that are closely related to polar codes, which the proposed 5G standard relies on. Furthermore, Aubry et al. [4] demonstrated how to generalize Reed-Muller codes to weighted projective Reed-Muller codes. Lachaud [9] created a metric for performance of codes that factors into account both the capability of a code to withstand errors, measured by the *relative distance* of the code, as well as the additional length needed to be added to the code, represented by the *transmission rate*. Based on this, Aubry et al. [4] calculated that weighted projective Reed-Muller codes had higher performances than both projective Reed-Muller codes and generalized Reed-Muller codes.

While weighted projective Reed-Muller codes have thus been empirically demonstrated to be higher-performing than both projective and generalized Reed-Muller codes, the performance of weighted projective Reed-Muller codes as a whole is not well-understood. While the transmission rate of the code is simple to calculate, the relative distance is dependent on the number of solutions to a hypersurface in weighted projective space over a finite field. Specifically, the more solutions such a hypersurface has, the lower the relative distance and thus the lower the performance of the code. This project focuses on providing an upper bound to the maximum number of solutions to such a hypersurface, and thus proving such a bound corresponds to knowing the worst-case performance of a weighted projective Reed-Muller code.

7 Conclusions and Further Research

We generalized the results of Aubry et al. [4] to Theorem 1, proving specific cases of Conjecture 1 for all dimensions m instead of only $m \leq 2$ as they proved. Moreover, we removed the divisibility conditions on d in Conjecture 1, resulting in Theorem 2 and Corollary 3 that address the $m \leq 2$ case in more generality than Conjecture 1. In addition, we proved in Theorem 4 that when $d \leq m$, the order of any hypersurface must satisfy the modular congruence $|V(F)| \equiv 1 \pmod{p}$.

For further research, one may generalize the results of Theorem 1 to a proof of Conjecture 1. In addition, one may expand and possibly strengthen the results of Theorem 2 and Corollary 3 to higher dimensions. Better understanding the specific values $|V(F)|$ can take by improving Theorem 4 to a proof of Conjecture 2 is also of interest. Finally, further investigating the distributions of $|V(F)|$ will also provide information that may be useful in improving the bounds and increasing the generality of Theorem 1.

Acknowledgements

I sincerely thank my mentor, Chun Hong Lo, of the Department of Mathematics at the Massachusetts Institute of Technology, for guiding me throughout the entire math research process as well as providing insights and new ideas in weighted projective space, finite fields, and algebraic geometry as a whole. I would also like to thank Dr. Tanya Khovanova, of the Department of Mathematics at the Massachusetts Institute of Technology, and Dr. John Rickert, of the Department of Mathematics at the Rose-Hulman Institute of Technology, for their advice throughout the research process. I also thank Professor David Jerison and Professor Ankur Moitra, of the Department of Mathematics at the Massachusetts Institute of Technology, for overseeing and advising the research project. I would like to thank my sponsors, Gilead Sciences, Inc., Mr. and Mrs. Brent T. Lin, and Mr. Jay Shankar and Ms. Niranjana Ravishankar. Finally, I would like to thank the Research Science Institute for an unparalleled and unique research opportunity, the Center for Excellence in Education for running the program, and the Massachusetts Institute of Technology, especially the Department of Mathematics.

References

[1] M. Datta and S. R. Ghorpade. On a conjecture of Tsfasman and an inequality of Serre for the number of points on hypersurfaces over finite fields. *arXiv preprint arXiv:1503.03049*, 2015.

[2] R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[3] J.-P. Serre. Lettre á M. Tsfasman du 24 juillet 1989. *Astérisque*, 198(200):351–353, 1991.

[4] Y. Aubry, W. Castryck, S. R. Ghorpade, G. Lachaud, M. E. O'Sullivan, and S. Ram. Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory. In *Algebraic Geometry for Coding Theory and Cryptography*, pages 25–61. Springer, 2017.

[5] M. Reid. Graded rings and varieties in weighted projective space. 2002.

[6] C. Delorme. Espaces projectifs anisotropes. *Bulletin de la Société Mathématique de France*, 103:203–223, 1975.

[7] J.-P. Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012.

[8] R. W. Hamming. Error detecting and error correcting codes. *The Bell system technical journal*, 29(2):147–160, 1950.

[9] G. Lachaud. The parameters of projective Reed–Müller codes. *Discrete Mathematics*, 81(2):217–221, 1990.

A Distributions of $|V(F)|$ for Fixed q, d, and $\vec{a}$

The following distributions of $|V(F)|$ for the specified values of q, d, and $\vec{a}$ were calculated using a complete search program in SageMath

q	deg	weights (a)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	1,1	1	3	3													
2	2	1,2	0	3														
2	2	1,1,1	0	7	0	35	0	21										
2	2	1,1,2	0	1	0	11	0	3										
2	2	1,2,2	0	0	0	7												
2	2	1,1,1,1	0	0	0	35	0	168	0	435	0	280	0	105				
2	2	1,1,1,2	0	0	0	7	0	0	0	99	0	0	0	21				
2	2	1,1,2,2	0	0	0	1	0	0	0	27	0	0	0	3				
2	2	1,2,2,2	0	0	0	0	0	0	0	15								
2	3	1,1	2	6	6	1												
2	3	1,3	0	3														
2	3	1,1,1	8	56	168	280	280	168	56	7								
2	3	1,1,3	0	2	0	22	0	6	0	1								
2	3	1,3,3	0	0	0	7												
2	3	1,1,1,3	0	8	0	56	0	168	0	1304	0	280	0	168	0	56	0	7
2	3	1,1,3,3	0	0	0	2	0	0	0	54	0	0	0	6	0	0	0	1
2	3	1,3,3,3	0	0	0	0	0	0	0	15								
2	4	1,1	4	12	12	3												
2	5	1,1	8	24	24	7												
2	6	1,1	16	48	48	15												
2	7	1,1	32	96	96	31												
2	8	1,1	64	192	192	63												
2	9	1,1	128	384	384	127												
3	2	1,1	3	4	6													
3	2	1,2	0	4														
3	2	1,1,1	0	39	0	0	247	0	0	78								
3	2	1,1,2	0	3	0	0	31	0	0	6								
3	2	1,2,2	0	0	0	0	13											
3	2	1,2,2,2	0	0	0	0	0	0	0	0	0	0	0	0	0	40		
3	3	1,1	8	16	12	4												
3	3	1,3	0	4														
3	3	1,1,3	0	8	0	0	97	0	0	12	0	0	4					
3	3	1,3,3	0	0	0	0	13											
3	3	1,3,3,3	0	0	0	0	0	0	0	0	0	0	0	0	0	40		
3	4	1,1	24	48	36	12	1											
3	4	1,2	3	4	6													
3	4	1,4	0	4														
3	4	1,1,2	81	348	810	1944	2235	2025	1458	684	81	162	12	0	0	1		
3	4	1,1,4	0	24	0	0	291	0	0	36	0	0	12	0	0	1		
3	4	1,2,2	0	39	0	0	247	0	0	78								
3	4	1,2,4	0	3	0	0	31	0	0	6								
3	4	1,4,4	0	0	0	0	13											
3	4	1,4,4,4	0	0	0	0	0	0	0	0	0	0	0	0	0	40		
4	2	1,2	0	5														
4	2	1,1,2	0	6	0	0	0	69	0	0	0	10						
4	2	1,2,2	0	0	0	0	0	21										
4	3	1,3	0	5														
4	3	1,1,3	0	20	0	0	0	291	0	0	0	20	0	0	0	10		
4	3	1,3,3	0	0	0	0	0	21										
4	4	1,2	6	5	10													
4	4	1,4	0	5														
4	4	1,2,2	0	126	0	0	0	1029	0	0	0	210						
4	4	1,2,4	0	6	0	0	0	69	0	0	0	10						
4	4	1,4,4	0	0	0	0	0	21										
5	4	1,2,4	0	10	0	0	0	0	131	0	0	0	0	15				
9	2	1,2,2	0	0	0	0	0	0	0	0	0	0	91					
9	5	1,5,5	0	0	0	0	0	0	0	0	0	0	91					

Table 1: Calculated Distributions of $|V(F)|$.